BARBARA SANDFUCHS

Privatheit wider Willen?

Internet und Gesellschaft
2

Mohr Siebeck

Internet und Gesellschaft

Schriften des Alexander von Humboldt Institut
für Internet und Gesellschaft

Herausgegeben von
Jeanette Hofmann, Ingolf Pernice,
Thomas Schildhauer und Wolfgang Schulz

2



Barbara Sandfuchs

Privatheit wider Willen?

Verhinderung informationeller Preisgabe im Internet nach deutschem und US-amerikanischem Verfassungsrecht

Mohr Siebeck

Barbara Sandfuchs, Studium der Rechtswissenschaft; ehrenamtliche Vollzeittätigkeit als Präsidentin der European Law Students' Association; 2012–2015 Promotion an der Universität Passau, DFG-Graduiertenkolleg Privatheit, Forschungsaufenthalte an der University of California at Berkeley, der Stanford University und der University of Pennsylvania; seit 2013 Lehrbeauftragte an der Universität Leipzig.

Veröffentlicht mit finanzieller Unterstützung der Universität Passau und des Oskar-Karl-Forster-Fonds.

e-ISBN PDF 978-3-16-154158-2
ISBN 978-3-16-154158-2
ISSN 2199-0344 (Internet und Gesellschaft)

Die Deutsche Nationalbibliothek verzeichnet diese Publikation in der Deutschen Nationalbibliographie; detaillierte bibliographische Daten sind im Internet über *http://dnb.dnb.de* abrufbar.

Das Buch wurde von Gulde-Druck in Tübingen gesetzt und auf alterungsbeständiges Werkdruckpapier gedruckt und gebunden.



Meiner Mutter

Vorwort

„Die Freiheit der Privatautonomie beim Datenschutz beinhaltet (…) die Möglichkeit eines ‚Paktes mit dem Teufel'".[1]

Thilo Weichert bringt das Kernproblem des Privatheitsschutzes im Online-Kontext auf den Punkt. Für die von digitalem Exhibitionismus beeinflusste Informationsgesellschaft ist es kennzeichnend, dass viele Bedrohungen für die informationelle Privatheit der Nutzer von diesen selbst ausgehen. Gleichzeitig ist ein solches selbstgefährdendes Verhalten Freiheitsausübung.

Wie müssen respektive können der deutsche und der US-amerikanische Staat auf als allzu großzügig empfundenes Preisgabeverhalten ihrer Bürger reagieren? Sind die Nutzer, überspitzt ausgedrückt, vor ihrer eigenen Dummheit zu schützen? Soll der Staat mitansehen, wie Nutzer Fehler begehen, die sie später bereuen werden? Oder gibt es einen Mittelweg, der die Entscheidungsautonomie der Nutzer respektiert und trotzdem eine gesamtgesellschaftlich bedenkenswerte Erosion der Privatheit verhindert?

Diesen Fragen geht die vorliegende Schrift nach, die aus meiner im Mai 2015 von der Juristischen Fakultät der Universität Passau angenommenen Dissertation hervorgegangen ist und sich auf dem Stand Juni 2015 befindet. Entstanden ist die Arbeit in meiner Zeit als Stipendiatin am DFG-Graduiertenkolleg 1681 „Privatheit" an der Universität Passau, während der ich das Privileg hatte, drei Forschungsaufenthalte in den USA absolvieren zu können.

Mein ganz besonderer Dank gilt meinem Doktorvater Prof. Dr. Gerrit Hornung, LL.M., der nicht nur früh mein Interesse für den Privatheitsschutz geweckt und mich zur Promotion ermutigt hat, sondern mir während der gesamten Bearbeitungszeit immer sofort, unkompliziert, geduldig, konstruktiv, vertrauensvoll und unterstützend zur Seite stand.

Prof. Dr. Dirk Heckmann danke ich sehr für die rasche Erstellung des Zweitgutachtens und die fruchtbare gemeinsame Zeit im Graduiertenkolleg, Prof. Dr. Ingolf Pernice für die freundliche Aufnahme in die Schriftenreihe „Internet und Gesellschaft" und Prof. Dr. Karsten Fitz für die hilfreiche interdisziplinäre Begleitung der Arbeit im Rahmen des Graduiertenkollegs.

Herzlich danken möchte ich auch Prof. Paul M. Schwartz für die Betreuung während meines Forschungsaufenthaltes an der University of California at Berkeley,

[1] *Weichert*, Datenschutz als Verbraucherschutz, in: Peissl (Hrsg.), Privacy, 2003, 145, 150.

Prof. Dr. Barbara van Schewick für die Begleitung am Stanford Center for Internet and Society, Prof. Dr. Anita L. Allen für die Einladung an die University of Pennsylvania und die sehr hilfreichen Diskussionen sowie Prof. Helen Nissenbaum für die Aufnahme in die Privacy Research Group an der New York University.

Zum Gelingen der Arbeit ganz entscheidend beigetragen hat die Förderung durch die Koordinatoren am Graduiertenkolleg, Dr. Stefan Halft, Henning Hofmann, Dr. Andreas Kapsner und Dr. Innokentij Kreknin. Für die treue wissenschaftliche Unterstützung und langjährige Freundschaft danke ich Dr. Wilfried Bernhardt. Ohne die beständigen Anregungen und Ermutigungen von Dr. Thomas Schwabenbauer wäre die vorliegende Arbeit nicht in dieser Form möglich gewesen, weshalb ich ihm ausgesprochen verbunden bin. Für den wissenschaftlichen Austausch und die freundschaftliche Unterstützung danke ich meinen Weggefährten im Graduiertenkolleg und insbesondere Dr. Matthias Herz, meinen Kollegen am Lehrstuhl sowie Franziska Greiner, Frank Ingenrieth, Jun. Prof. Dr. Lars Hornuf und Dorothee Lang.

Dankbar bin ich weiter für die Unterstützung der Deutschen Forschungsgemeinschaft und der Kanzlei Gibson Dunn.

Eine besondere Ehre ist es schließlich, dass die Arbeit mit dem Wissenschaftspreis 2015 der Deutschen Stiftung für Recht und Informatik ausgezeichnet wurde.

Schließlich gilt meine größte Dankbarkeit Francisco, meiner Familie und meinen Freunden, die mir während Freud und Leid der Promotionszeit Rückhalt gegeben haben.

München, im Juli 2015 *Dr. Barbara Sandfuchs*

Abstract

Personenbezogene Daten werden von Internetnutzern freiwillig in implizierter und expliziter Weise preisgegeben. Dabei stellt die Nichtinanspruchnahme des Rechts, selbst zu bestimmen, wer wann was bei welcher Gelegenheit über die Einzelnen weiß, eine sowohl in Deutschland als auch in den Vereinigten Staaten von Amerika grundrechtlich geschützte Freiheitsausübung dar.

Ungeachtet etwaiger Vorteile einer informationellen Preisgabe können durch sie Gefahren für die Persönlichkeitsentwicklung der Nutzer sowie für Allgemeinwohlbelange entstehen, wenn beispielsweise der Kontrollverlust über die eigenen Daten langfristig zu Selbstzensur führt. Es kann daher gerade bei besonders sensiblen Daten oder wenig selbstbestimmten Preisgabesituationen ein Bedürfnis zur Verhinderung informationeller Preisgabe bestehen.

Mögliche, gleichermaßen in Deutschland und den Vereinigten Staaten von Amerika diskutierte, Mittel hierfür können ein erzwungener Schutz (also insbesondere Verbote), die Unterstützung informationellen Selbstschutzes (also insbesondere die Unterrichtung und die Ermöglichung technischen Selbstschutzes) sowie sogenannte Entscheidungsarchitekturen[2] (also gezielte Verhaltensbeeinflussung durch Ausnutzung vorhersehbarer Irrationalitäten) sein. Soweit entsprechende Maßnahmen in Nutzerrechte und die Rechte der verantwortlichen Stellen eingreifen, bedürfen sie der verfassungsrechtlichen Rechtfertigung.

Die Arbeit ist unterteilt in aus Schutzpflicht-Gesichtspunkten gebotene sowie rechtfertigbare, rechtspolitisch wünschenswerte Maßnahmen. Dafür wird zum einen nach den Zielen, zum anderen nach Geeignetheit und Eingriffsintensität der jeweiligen Intervention differenziert.

Auf Basis dieser Analyse wird das Konzept des partiellen informationellen Selbstschutzes herausgearbeitet. Dieses kann sowohl in Deutschland als auch in den USA einen sachgerechten Rahmen zur Verhinderung bestimmter informationeller Preisgabe bieten.

---

[2] Zu dem, maßgeblich von *Sunstein* und *Thaler* geprägten, Konzept ausführlich unten, siehe Kap. 4 c. Auch die deutsche Bundesregierung zeigt nun Interesse an dieser Form der Bürgerbeeinflussung, siehe *Hoffmann*, Politik per Psychotrick, 11.3.2015.

Inhaltsverzeichnis

Kapitel 1

Einleitung

„Was ist Privatheit, Privacy oder Privatsphäre? Diese Frage lässt sich nicht ohne Weiteres beantworten […]. Angesichts dessen muss man sich freilich doch mit Zweifeln daran auseinandersetzen, ob es sinnvoll und zweckmäßig ist, Privatheit – als ein Modell mittleren Abstraktionsgrades – zum Gegenstand des [figurativen] Forschungsexperiments zu machen.“[1]

Der Versuch sei gewagt.

A. Problemaufriss

Informationelle Preisgabe im Internet kann trotz ihrer positiven Seiten[2] mitunter Ausmaße und Ausprägungen annehmen, die für die Nutzer selbst und die Allgemeinheit gefährlich sind. Es kann daher nach Abwägung im Einzelfall sinnvoll erscheinen, bestimmte Preisgaben zu verhindern und so die Nutzer und ihre Umwelt zu schützen. Jedenfalls bei besonders sensiblen Daten oder im Falle von besonders gefährlichen Umständen der Preisgabe kann das rechtspolitische Bedürfnis bestehen, nicht erschließbare Privaträume zu definieren. Die Devise kann lauten: „Caring about not caring about privacy“.[3]

Muss oder kann der Staat Nutzer daran hindern, ihre genetischen Daten im Internet preiszugeben[4] oder Videoaufnahmen sadomasochistischer Praktiken auf Inter-

---

[1] *Rüpke*, Der verfassungsrechtliche Schutz der Privatheit, 1976, 27.

[2] Selbstredend kann die Preisgabe auch vielfältige Vorteile mit sich bringen. Diese können den Preisgebenden zugutekommen, beispielsweise durch Komfortgewinne im Alltagsleben oder durch die Möglichkeit zur Nutzung entgeltfreier Online-Angebote. Weiter können auch Vorteile für die Allgemeinheit entstehen, wenn beispielsweise die Ausbreitung von Grippewellen anhand der Analyse von Suchmaschinenanfragen nach Grippemedikamenten et cetera vorhergesagt wird: http://www.google.org/flutrends/about/how.html. Diese Chancen der Preisgabe sind im Einzelfall gegen die Nachteile abzuwägen. Beispiele für wissenschaftlichen Erkenntnisgewinn nennen: *Polonetsky/Tene*, Privacy and Big Data, 66 Stanford L. Rev. Online (2013), 25 ff. Einen Einblick in die Vielzahl der Möglichkeiten bieten: *Mayer-Schönberger/Cukier*, Big Data, 2013. Ein Plädoyer für Vertrauen in die kulturelle Eigendynamik von Onlineprozessen liefert: *Lutterbeck*, Komplexe Kontexte – einfache Regeln, in: Mehde/Ramsauer/Seckelmann (Hrsg.), Staat, Verwaltung, Information, 2011, 1017 ff.

[3] *Allen*, Unpopular Privacy, 2011, 171; zu den aus der „Sorglosigkeit“ der Nutzer erwachsenden Fragen, siehe auch: *Heckmann*, Öffentliche Privatheit, K&R 2010, 770, 772.

[4] Beispielsweise über die Webseite: http://genomesunzipped.org/.

net-Plattformen hochzuladen? Muss oder kann er sie davon abhalten, umfassende Einwilligungen zu Datenerhebungen, -verarbeitungen und -nutzungen zu geben, wenn die daraufhin entstehenden Persönlichkeitsprofile ihnen langfristig gesehen großen Schaden zufügen können?

Was ist, wenn der Staat die Nutzer nicht hindert, sondern den verantwortlichen Stellen nur eine Unterrichtungspflicht auferlegt? Oder wenn er Webseitenanbieter verpflichtet, einen die Nutzer verfolgenden Avatar anzuzeigen, den die Nutzer mit einem Klick ausblenden oder aber ihr Opt-out aus dem Tracking erklären können?[5]

Und wie wirkt es sich auf die rechtliche Bewertung aus, wenn die Nutzer minderjährig sind oder die Videomitschnitte sadomasochistischer Praktiken auch den Partner zeigen?

Die aufgeworfenen Fragen geben Einblick in die Brisanz, die der Verhinderung informationeller Preisgabe im Internet zukommt. Dabei ist die Selbstentblößung durch die Einzelnen keineswegs ein neues Problem, sondern wird beispielsweise schon 1967 in *Westins* grundlegendem Werk „Privacy and Freedom“ zum Anlass genommen, über Wert und Schutz der Privatheit nachzudenken.[6] Im Zeitalter des „homo facebook“[7] bietet das Internet potenzierte Möglichkeiten zur informationellen Preisgabe, wodurch eine Vielzahl an privaten Akteuren Zugriff auf die Daten der Nutzer erhält. Zusätzlich können Strafverfolgungsbehörden und Geheimdienste im In- und Ausland unter für die Einzelnen schwer über- und durchschaubaren rechtlichen Voraussetzungen Zugang zu privaten Datensammlungen erhalten. So entstehen für die Nutzer durch informationelle Preisgabe nicht nur Bedrohungen in Form der Datenauswertung durch Private, sondern auch durch die Datenanalyse staatlicher Stellen im In- und Ausland.[8] Es stellt sich daher aktuell umso mehr die Frage nach dem Schutz vor diesen Gefahren.

Ein staatliches Untätigbleiben im bloßen Vertrauen auf die Selbstregulierung des Markts und die Rationalität seiner Teilnehmer erscheint ebenso problematisch wie eine vollständige „Datenaskese“[9] als Verzicht auf jegliche Datenpreisgabe. Nicht zu unterschätzen ist der, auch dem in § 3a BDSG normierten Gebot der Datenvermeidung und -sparsamkeit zugrunde liegende, Gedanke, dass einmal preisgegebene Daten der Kontrolle der Einzelnen weitgehend entzogen sind.[10] Die Zurückerlangung oder Sperrung der Daten ist technisch in aller Regel unmöglich und rechtlich außerhalb des Geltungsbereichs[11] des europäischen Datenschutzrechts de facto

[5] Ein solches Vorgehen wird vorgeschlagen von: *Calo*, Against Notice Skepticism in Privacy (and Elsewhere), 87 Notre Dame L. Rev. (2012), 1027, 1040.

[6] *Westin*, Privacy and Freedom, 1967, 52 ff.

[7] *Worms/Gusy*, Verfassung und Datenschutz, DuD 2012, 92, 96.

[8] Während den Nutzern Rechtsschutzmöglichkeiten gegen Grundrechtseingriffe durch inländische staatliche Stellen zustehen, sind sie gegenüber ausländischen Stellen häufig, jedenfalls de facto, schutzlos.

[9] *Bull*, Zweifelsfragen um die informationelle Selbstbestimmung, NJW 2006, 1617 ff.

[10] *Scholz*, in: Simitis (Hrsg.), Bundesdatenschutzgesetz, 2014, § 3a, Rn. 12.

[11] Art. 4 der Richtlinie 95/46/EG des Europäischen Parlaments und des Rates v. 24.10.1995 zum

chancenlos. Ein sinnvoller Ansatzpunkt zur Verhinderung der mit informationeller Preisgabe verbundenen Gefahren kann daher insbesondere Prävention sein.[12]

Jedoch könnte den Nutzern im Rahmen ihrer Persönlichkeitsentfaltung das Recht zustehen, selbst und eigenverantwortlich personenbezogene Daten im Internet preiszugeben, auch wenn daraus Gefahren für sie selbst erwachsen. So stellt *Der Spiegel* jüngst in einem Leitartikel fest: „Es ist die Selbstbestimmung, die am Ende die Selbstbestimmung gefährdet".[13]

Häufig mag ein Schutz den Nutzern sogar zugutekommen, da die Preisgabe für sie objektiv nachteilig gewesen wäre. Einer freiheitlichen Demokratie scheint es jedoch grundsätzlich versagt zu sein, die selbstbestimmt Handelnden nur um ihrer selbst willen paternalistisch zu bevormunden. Die Frage, ob dennoch staatliche Möglichkeiten und vielleicht sogar Pflichten bestehen, selbstbestimmte informationelle Preisgabe einzugrenzen, wird Gegenstand der folgenden Analyse sein.

B. Unzulänglichkeit nationalstaatlicher Betrachtung und faktischer Einfluss der USA

Aus der Natur der Informationsgesellschaft folgt, dass Grundrechtsfragen sich zwar im nationalen Bereich stellen, aber nicht ausschließlich im nationalen Kontext lösen lassen. Vielmehr bringt die weltweite Vernetzung neue Rechtsprobleme mit sich und fordert internationale Lösungsansätze. Als Standort der Mehrzahl der großen Akteure der Informationsgesellschaft, wie Apple Inc., Google Inc., Microsoft Inc. oder Facebook Inc., kommt den Vereinigten Staaten von Amerika eine bedeutende Rolle im Privatheitsschutz der Nutzer weltweit zu. Zugleich verspricht die dort hitzig geführte Diskussion über die Etablierung weitergehender datenschutzrechtlicher Standards Impulse auch für die Debatte diesseits des Atlantiks. Die Arbeit nimmt daher neben der deutschen auch die US-amerikanische (Bundes-)[14]Verfassungsordnung in den Blick.

Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr, im Folgenden abgekürzt als: DSRL; dazu EuGH EuZW 2014, 541 (544); für das Bundesdatenschutzgesetz: § 1 Abs. 2, 5 BDSG; *Berger/Kraska*, Datenschutz im Web 2.0, 2012 und *Hornung*, Europa und darüber hinaus, in: Hill/Schliesky (Hrsg.), Die Neubestimmung der Privatheit, 2014, 123, 130 f.

[12] So auch: *Hansen*, Privacy Enhancing Technologies, in: Roßnagel (Hrsg.), Handbuch Datenschutzrecht, 2003, 291, 305, Rn. 46 und *Roßnagel/Pfitzmann/Garstka*, Modernisierung des Datenschutzrechts, 2001, 37, 101 ff., 148.

[13] *Der Spiegel*, Kampf den Avataren, Ausgabe 21/2014, 12. In diese Richtung geht auch *Hoffmann-Riem*, wenn er feststellt, dass sich die Einwilligung als „Prototyp eines Instruments der Selbstbestimmung" im Ergebnis gegen diese Selbstbestimmung wende: *Hoffmann-Riem*, Freiheitsschutz in den globalen Kommunikationsinfrastrukturen, JZ 2014, 53, 54.

[14] Den US-Bundesstaaten kommt eine weit größere Eigenständigkeit zu als den deutschen Bundesländern. Die Arbeit konzentriert sich auf das deutsche Grundgesetz und die US-Bundesverfas-

Zudem befasst sich der wissenschaftliche Diskurs in Deutschland nicht allein mit dem hergebrachten Privatheitsverständnis des deutschen Verfassungsrechts.[15] Vielmehr reicht der Blick über den Tellerrand hinaus und berücksichtigt angloamerikanische, insbesondere aus den USA stammende Forschungsansätze.[16] Während in der außer-juristischen Literatur trotz Bedeutungsunterschieden[17] Privatheit und der in der englischsprachigen Literatur gebrauchte Begriff Privacy häufig gleichgesetzt werden (müssen), um einen internationalen Austausch zu ermöglichen, haben aus juristischer Sicht zahlreiche Arbeiten die rechtsvergleichende Analyse beider Konzepte zum Gegenstand.[18] Ein Einblick in das Privacy-Verständnis, wie es in der US-Rechtsordnung zum Ausdruck kommt, ist unerlässlich, um einen beträchtlichen Teil der international relevanten Forschung erschließen zu können. Wie sich zeigen wird, misst jedenfalls die US-amerikanische Literatur der Information(al)[19] Privacy eben jenen über die Individuen hinausgehenden Wert zu, den die deutsche Verfassungsordnung für die informationelle Privatheit zugrunde legt.[20] Trotz der verschiedenen Ausgangslagen erscheint es daher häufig möglich, jedenfalls die Begriffe informationelle Privatheit und Informational Privacy gleichzusetzen.

C. Ziel der Arbeit

Denkbarer Anlass[21] und gleichsam Tertium Comparationis zwischen der deutschen und der US-amerikanischen Rechtslage ist das rechtspolitische Bedürfnis, be-

---

sung. Soweit dies zusätzliche Erkenntnisse verspricht, wird in einem Exkurs auf einzelstaatliche Verfassungsordnungen eingegangen.

[15] Siehe insbesondere unten Kapitel 3,B.I.1.

[16] Nach *Schiedermair* wird der Schutz der Privatheit in den USA sogar intensiver diskutiert als in Deutschland: *Schiedermair*, Der Schutz des Privaten als internationales Grundrecht, 2012, 17. Dem ist insofern zuzustimmen, als dort derzeit aufgrund der nur eingeschränkten verfassungsrechtlichen Absicherung informationeller Privatheit ein intensiver Diskurs zum wünschenswerten Privatheits-Schutzniveau geführt wird.

[17] Ausführlich dazu: *Schwartz*, Das Übersetzen im Datenschutzrecht, in: Frank/Maaß/Paul (Hrsg.), Übersetzen, verstehen, Brücken bauen, 1993, Bd. 1, 366 ff.

[18] Beispielsweise: *Amelung*, Der Schutz der Privatheit im Zivilrecht, 2002; *Buchner*, Informationelle Selbstbestimmung im Privatrecht, 2006; *Genz*, Datenschutz in Europa und den USA, 2004; *Kamlah*, Right of Privacy, 1969; *Wittern*, Das Verhältnis von Right of Privacy und Persönlichkeitsrecht zur Freiheit der Massenmedien, 2004; eine ausführliche deutschsprachige Darstellung der US-Grundrechtsdogmatik (ohne Rechtsvergleich) bietet: *Brugger*, Grundrechte und Verfassungsgerichtsbarkeit in den Vereinigten Staaten von Amerika, 1987 und *ders.*, Angloamerikanischer Einfluss auf die Grundrechtsentwicklung in Deutschland, in: Isensee/Kirchhof (Hrsg.), Handbuch des Staatsrechts der Bundesrepublik Deutschland X, 2012, 121 ff.

[19] In der Literatur findet sich neben der Bezeichnung „Informational Privacy" gelegentlich auch der Begriff „Information Privacy". Beide werden gleichbedeutend verwendet, in Rahmen dieser Arbeit soll der Einheitlichkeit halber von „Informational Privacy" gesprochen werden.

[20] Siehe insbesondere unten Kapitel 3,A.III.

[21] Zur Herleitung dieses Anlasses, siehe unten: Kapitel 3.

stimmte Formen von informationeller Preisgabe im Internet zu verhindern, um ihren Gefahren vorzubeugen.

Im Verlauf dieser Arbeit wird ein rechtspolitischer Weg gesucht, besonders gefährlicher informationeller Preisgaben zu begegnen, ohne dabei übermäßig in die Rechte der Preisgebenden und in die Rechte der verantwortlichen Stellen einzugreifen.

Dabei werden die Lösungsmöglichkeiten nach deutschem und US-amerikanischem Verfassungsrecht analysiert, die Gemeinsamkeiten und Unterschiede herausgearbeitet und nach den Gründen für die Kontraste gefragt. So sollen die für Deutschland beste Lösung erkannt und rechtspolitische Folgerungen gezogen werden. Gleichzeitig wird bezweckt, einen Beitrag zum gegenseitigen Verständnis zu leisten und so die gemeinsame Festlegung privatheitsfördernder Standards zu unterstützen.

Ziel ist damit eine verfassungsrechtliche Systematisierung der bestehenden Möglichkeiten zur Verhinderung informationeller Preisgabe im Internet und der hierfür heranziehbaren Rechtfertigungsgründe. Dadurch soll der Blick eröffnet werden für eine grundlegende Schutzstruktur, die als Basis für kommende Forschung und einfachgesetzliche Umsetzung dienen kann.

D. Gang der Untersuchung

Ausgehend von der Definition des Schlüsselbegriffs informationelle Preisgabe (siehe Kapitel 2) werden die durch informationelle Preisgabe im Internet gefährdeten Rechtsgüter analysiert. Dabei werden zunächst die tatsächlichen Gefahren dargestellt, bevor diese Rechtsgütern zugeordnet werden, die jeweils im deutschen und US-amerikanischen Recht Schutz erfahren (siehe Kapitel 3). Im Anschluss werden die denkbaren Maßnahmen zur Verhinderung informationeller Preisgabe in die drei Kategorien erzwungener Schutz, Unterstützung informationellen Selbstschutzes und Schutz durch (im Bereich der Verhaltensökonomie diskutierte) Entscheidungsarchitekturen eingeteilt (siehe Kapitel 4).

Der Stellenwert, den die beiden Verfassungen jeweils den bedrohten Gütern zuordnen, ist dann Grundlage für die Prüfung, ob die Staaten zum Schutz dieser Güter informationelle Preisgabe verhindern müssen (siehe Kapitel 5). Weiter ist deren Gewicht dafür entscheidend, ob das bedrohte Gut jeweils bedeutend genug ist, zu seinem Schutz die Preisgabe verhindern zu dürfen (siehe Kapitel 6).

Die im Rahmen dieser Analyse gefundenen Gemeinsamkeiten und Unterschiede werden dann zum Anlass genommen, nach zukünftigen verfassungskonformen Wegen zur Verhinderung informationeller Preisgabe zu fragen. Dabei wird zunächst das Konzept des insbesondere in den Vereinigten Staaten diskutierten libertären Paternalismus analysiert (siehe Kapitel 7,A), bevor der eigene Ansatz des par-

tiellen informationellen Selbstschutzes ausgearbeitet wird (siehe Kapitel 7, B) Schließlich werden die Ergebnisse zusammengefasst (siehe Kapitel 8).

Kapitel 2

Definition informationeller Preisgabe

Der Terminus informationelle Preisgabe wird im Rahmen dieser Arbeit verstanden als die langfristige Aufgabe eigener informationeller Privatheit durch die Privatheitsträger selbst. Diese – als Oxymoron anmutende – Definition bringt das Kernproblem der hier untersuchten Fragestellung auf den Punkt: Jede Privatheitsaufgabe ist kurzfristig gesehen auch Privatheitsausübung. Die Entscheidung zur Preisgabe personenbezogener Daten stellt zum Zeitpunkt der Preisgabe eine Ausübung der Privatheit dar. Gleichzeitig führt sie dazu, dass auf längere Sicht keine Privatheit mehr besteht, da die Betroffenen nun über die Preisgabe ihrer – bereits preisgegebenen – Daten nicht mehr bestimmen können.

Es gilt, sowohl die (informationelle) Privatheit als den Gegenstand der Preisgabe (siehe A) als auch den Akt der Preisgabe durch die Privatheitsträger selbst zu beleuchten (siehe B).

A. Informationelle Privatheit

Neben der informationellen Privatheit werden häufig eine Reihe anderer Aspekte ausgemacht, die gemeinsam als Privatheit bezeichnet werden. Dieser Zusammenhang soll im Folgenden untersucht werden. Der Begriff Privatheit ist schillernd, die vorhandenen Deutungsversuche hinsichtlich seines Sinngehalts gehen weit auseinander.[1] Hierzu wird in der Literatur festgestellt: „the concept of privacy is embarrassingly difficult to define. [… F]undamentally important though it may be, [it] is an unusually slippery concept."[2]

---

[1] Einen Überblick über historische Entwicklungen und aktuelle Debatten geben: *Bull*, Netzpolitik, 2013, 49; *Schiedermair*, Der Schutz des Privaten als internationales Grundrecht, 2012, 23 ff.; *Schwabenbauer*, Heimliche Grundrechtseingriffe, 2013, 91 ff. und *Wolff*, Privatheit und Öffentlichkeit, in: Hill/Martini/Wagner (Hrsg.), Facebook, Google & Co., 2013, 19 ff. *Posner* führt zutreffend aus: „The concept of ‚privacy' is elusive and ill defined. Much ink has been spilled in trying to clarify its meaning.", *Posner*, The Right of Privacy, 12 Georgia L. Rev. (1978), 393.

[2] *Whitman*, The Two Western Cultures of Privacy, 113 Yale L. J. (2004), 1151, 1153.

I. Funktionaler Wert

Jedenfalls wird Privatheit regelmäßig als untrennbar verknüpft angesehen mit der Sicherung von Autonomie.[3] Im Kern dient Privatheit demnach der Freiheit der Individuen, ihr Leben in liberal-demokratischen Grenzen, also insbesondere unter Achtung der gleichen Freiheit Anderer, frei von äußeren Einflüssen gestalten zu können. Privat ist, was um der Sicherung der personalen Autonomie der Einzelnen willen Andere nichts anzugehen hat.[4] „Wieviel Freiheit der einzelne in einer Gesellschaft genießt, bemißt sich daran, ob er sein Leben auf die ihm eigene Weise zu führen vermag, ohne daß sich unerbeten Dritte einmischen. Privatheit ist das Fundament der Freiheit, und diese Freiheit schützt vor jedweder Macht."[5] Individuen definieren ihre Rolle und ihr Verhältnis zur Umwelt selbst. Sie können sich die Frage stellen, wer sie sein möchten, wie sie leben möchten und ihr Leben entsprechend gestalten.[6] Entsprechend setzt auch das Bundesverfassungsgericht einen Zusammenhang von Privatheit und Entscheidungsfreiheit sowie von Privatheit und Verhaltensfreiheit voraus.[7] Die Privatheit dient demnach dazu, den Individuen Autonomie zu gewährleisten.

Privatheit als Mittel zur Sicherung von Selbstbestimmung kann über den Weg der Zugangs- und Kontrollbereiche definiert werden.[8] So bezeichnet *Rössler* etwas als privat, wenn man selbst den Zugang zu diesem Etwas kontrollieren kann.[9] Durch das Charakteristikum der Kontrolle wird deutlich, dass Privatheit zum einen nicht identisch ist mit dem Zustand des Abgeschottetseins und dass die Zugänglichkeitsgrenzen zum anderen relativer Natur sind.[10] Staatliche Schutzaufträge können daher unter anderem darauf gerichtet sein, die Individuen vor unerwünschtem oder unberechtigtem Zugang zu bewahren, wobei dem Zugang sowohl räumliche als vor allem auch übertragene Bedeutung im Sinne von Kenntnisnahme zukommt.[11] Der Zugangsschutz ist dabei vielfältig: „privacy is control over when and by whom the

---

[3] *Rössler*, Privatheit, in: Gosepath/Hinsch/Rössler (Hrsg.), Handbuch der Politischen Philosophie und Sozialphilosophie, 2008, 1023, 1028.

[4] *Horn*, Schutz der Privatsphäre, in: Isensee/Kirchhof (Hrsg.), Handbuch des Staatsrechts der Bundesrepublik Deutschland VII, 2009, 147, 162.

[5] *Sofsky*, Verteidigung des Privaten, 2009, 149.

[6] *Rössler*, Der Wert des Privaten, 2001, 39, 83, 97 ff.

[7] In genannter Reihenfolge: BVerfGE 118, 168 (198) und 120, 180 (197).

[8] Vgl. *Horn*, Schutz der Privatsphäre, in: Isensee/Kirchhof (Hrsg.), Handbuch des Staatsrechts der Bundesrepublik Deutschland VII, 2009, 147, 156; *Moore*, Privacy, 40 American Philosophical Quarterly (2003), 215, 216; dagegen: *Thomson*, The Right to Privacy, 4 Philosophy & Public Affairs (1975), 295, 305, Fn. 1: „If my neighbor invents an X-ray device which enables him to look through walls, then I should imagine I thereby lose control over who can look at me: going home and closing the doors no longer suffices to prevent others from doing so. But my right to privacy is not violated until my neighbor actually does train the device on the wall of my house. It is the actual looking that violates it, not the acquisition of power to look."

[9] *Rössler*, Der Wert des Privaten, 2001, 23.

[10] *Albers*, Grundrechtsschutz der Privatheit, DVBl. 2010, 1061, 1062.

[11] *Rössler*, Der Wert des Privaten, 2001, 23.

various parts of us can be sensed by others. By ‚sensed', is meant simply seen, heard, touched, smelled, or tasted. By ‚parts of us', is meant the parts of our bodies, our voices, and the products of our bodies. ‚Parts of us' also includes objects very closely associated with us. By ‚closely associated' is meant primarily what is spatially associated. The objects which are ‚parts of us' are objects we usually keep with us or locked up in a place accessible only to us."[12] Privatheitsschutz wird damit umschrieben als Schutz der Kontrolle über das Private.[13]

Die dargestellte autonomie-orientierte Herangehensweise überzeugt, da sie eine sinnvolle Zuordnung verschiedenster Aspekte zu dem Oberbegriff Privatheit zulässt, solange diese der Autonomie-Sicherung dienen. Unter Operationalisierung dieses Privatheitsverständnisses wird daher im Rahmen der vorliegenden Arbeit alles als privat angesehen, was die Privatheitsträger aus beliebigen Gründen nicht zeigen möchten.

II. Drei Dimensionen nach Rössler

Aus nicht-rechtlicher Sicht[14] kann die Bedeutung der Privatheit in Anlehnung an die weithin anerkannte und inhaltlich überzeugende Systematisierung von *Rössler* aufgefächert werden in drei Dimensionen: die lokale, die dezisionale und die informationelle Privatheit.[15]

Der Ausgangspunkt für die Betrachtung der Debatte ist der lokale, also häusliche Bereich der Individuen. Entsprechend wird die lokale Privatheit sogar als das „Paradigma von Privatheit" bezeichnet.[16] Von einem gesicherten Bereich aus entfalten die Einzelnen ihr Leben und Wirken und sind dort nur zusammen mit denjenigen Menschen, mit denen sie sich verbunden fühlen.[17] Außerhalb dieses Bereichs treten sie zwangsläufig in Interaktion mit ihrer Umwelt; innerhalb grundsätzlich nur, wenn sie dies selbst bestimmen. Der geschützte Raum, mag er auch noch so klein sein, bietet den Individuen Rückzugsmöglichkeiten und selbstbestimmte Herrschaftsgewalt. Es gelten die geflügelten Worten: My home is my castle. Die Zugangskontrolle zu den Räumen steht den Einzelnen ebenso zu wie die Möglichkeit zur Inszenierung des Rauminneren.[18] Auch nach Ansicht des Bundesverfassungsgerichts bedürfen die Einzelnen eines Raumes, in dem sie die Möglichkeit haben,

---

[12] *Parker*, A Definition of Privacy, 27 Rutgers L. Rev. (1974), 275, 281. Angesichts der Bedeutung der Kontrolle über personenbezogene Daten für das Individum wird man auch diese als vom Schutz erfasst ansehen müssen.

[13] *Horn*, Schutz der Privatsphäre, in: Isensee/Kirchhof (Hrsg.), Handbuch des Staatsrechts der Bundesrepublik Deutschland VII, 2009, 147 ff.

[14] Aus rechtlicher Sicht lassen sich diese Dimensionen verschiedenen Grundrechten zuordnen, siehe dazu für Deutschland unter Kapitel 3,B und für die Vereinigten Staaten unter Kapitel 3,C.

[15] *Rössler*, Der Wert des Privaten, 2001.

[16] *Nagenborg*, Diskretion in offenen Netzen, in: Spinner/Nagenborg/Weber (Hrsg.), Bausteine zu einer neuen Informationsethik, 2001, 93, 96.

[17] *Hohmann-Dennhardt*, Freiräume, NJW 2006, 545, 546.

[18] *Rössler*, Der Wert des Privaten, 2001, 257.

frei von öffentlicher Beobachtung und damit von der von ihr erzwungenen Selbstkontrolle zu sein. Bestünden solche Rückzugsbereiche nicht, könnten die Einzelnen psychisch überfordert sein, weil sie unausgesetzt darauf achten müssten, wie sie auf Andere wirken und ob sie sich richtig verhalten. Ihnen fehlten dann die Phasen des Alleinseins und Ausgleichs, die für die Persönlichkeitsentfaltung notwendig sind und ohne die sie nachhaltig beeinträchtigt würde.[19]

Weiter besteht die dezisionale Privatheit. Dieser kommt nach *Rössler* die Bedeutung eines individuellen Handlungsspielraums von Subjekten in all ihren sozialen Beziehungen zu, ein Handlungs- und Entscheidungsspielraum, der allererste individuelle Lebensentwürfe ermöglichen, erschließen und sichern kann.[20] Der selbst nur symbolische Zugang Anderer in jedweder Form kann nur durch die Individuen selbst kontrolliert werden.[21] Privatheit wird somit die Bedeutung der Freiheit von Rechtsfertigungszwängen zugewiesen.[22] Den Individuen wird die Autonomie eingeräumt, nach eigenem Belieben andere von Angelegenheiten auszuschließen, schlicht mit der Begründung, diese seien Privatsache.[23]

Schließlich bleibt noch die Kategorie der informationellen Privatheit, die die Kontrolle darüber beinhaltet, „wer was wie über eine Person weiß".[24]

III. Vertiefung: Informationelle Privatheit

Der Schwerpunkt dieser Arbeit liegt auf den letztgenannten Aspekten der Privatheit. Diese fallen nach *Rössler* unter die Dimension der informationellen Privatheit, werden in Deutschland nach herkömmlichem Verständnis durch das Recht auf informationelle Selbstbestimmung geschützt und in den USA als Informational Privacy bezeichnet.

Unter informationeller Privatheit soll im Folgenden in Anlehnung an das sogenannte Volkszählungsurteil des Bundesverfassungsgerichts[25] die tatsächliche Möglichkeit der Einzelnen zur informationelle Selbstbestimmung und damit zur Entscheidung über die Preisgabe und Verwendung der eigenen personenbezogenen Daten verstanden werden. Die genaue Festlegung dessen, was unter personenbezogenen Daten zu verstehen ist, ist umstritten.[26] Wenn im Rahmen dieser Arbeit ver-

[19] BVerfGE 101, 361 (383).

[20] *Rössler*, Der Wert des Privaten, 2001, 169.

[21] *Rössler*, Der Wert des Privaten, 2001, 144.

[22] *Rössler*, Der Wert des Privaten, 2001, 161 f.

[23] *Rössler*, Der Wert des Privaten, 2001, 144.

[24] *Rössler*, Der Wert des Privaten, 2001, 201.

[25] BVerfGE 65, 1 (43). Das Recht auf informationelle Selbstbestimmung wird daher im Kontext dieser Arbeit bedeutungsgleich mit einem „Recht auf informationelle Privatheit" verwendet. Der Terminus „informationelle Privatheit" beschreibt die tatsächliche Möglichkeit zur informationelle Selbstbestimmung.

[26] Zu den folgenden und weiteren Definitionsansätzen: *Schwartz/Solove*, The PII Problem, 86 New York Univ. L. Rev. (2011), 1814, 1828 ff.; *dies.*, Reconciling Personal Information in the United States and European Union, UC Berkeley Public Law Research Paper, 2271442, 20 ff. und

kürzt von Daten die Rede ist, bezieht sich dies auf die Definition nach § 3 Abs. 1 BDSG, also auf „Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbaren natürlichen Person." Uneinigkeit besteht insoweit darüber, ob die Bestimmung nur abstrakt irgendjemandem möglich sein muss (absolute Theorie) oder ob auf die Bestimmbarkeit durch diejenigen abzustellen ist, die jeweils über das noch unbestimmte Datum verfügen (relative Theorie).[27] Aus Gründen des Schutzzwecks und der Praktikabilität erscheint es sachgerecht, einen Mittelweg zu gehen und auf die Bestimmbarkeit durch die speichernde Stelle abzustellen, wobei jedoch auch die Informationen miteinbezogen werden müssen, die sich die Stelle ohne übermäßigen Aufwand beschaffen kann.[28] Bei der Frage, welche Schutzpflichten und welche Möglichkeiten zur Verhinderung der Preisgabe bestehen, wird auch berücksichtigt werden müssen, wie hoch die Wahrscheinlichkeit der Herstellung eines Personenbezugs im konkreten Fall ist.

Terminologisch wird in der Literatur zutreffenderweise zwischen Daten und Informationen unterschieden. Dritte können aus Daten kontextbezogen Informationen gewinnen. Diese Informationen stellen Sinnelemente dar, die erst aufgrund der Leistung der Dritten entstehen.[29] Die Zugangsbeschränkung durch die Individuen bezieht sich nur auf deren Daten. Indem sie kontrollieren, welche Daten Anderen zur Verfügung gestellt werden, können sie die über sie gewonnenen Informationen beeinflussen. So können sie wissen oder jedenfalls abschätzen, wer wann über welche sie betreffenden Informationen verfügt und sich entsprechend verhalten beziehungsweise Gegenmaßnahmen einleiten. Von der informationellen Privatheit erfasst ist auch das Wissen darüber, woher Andere die Daten bezogen haben und in welcher Beziehung die Anderen somit zu den Individuen stehen.[30] Impliziert ist somit die „Kontrolle über die Selbstdarstellung"[31], die die Einzelnen erreichen, indem sie ausgewählte personenbezogene Daten an von ihnen bestimmte Adressaten zu bestimmten Verwendungen preisgeben.

Die vorliegende Arbeit verwendet den Begriff der informationellen Privatheit, da er anschlussfähig an die in den USA geführte Privatheits-Diskussion ist, auch in

---

Tinnefeld, Geschützte Daten, in: Roßnagel (Hrsg.), Handbuch Datenschutzrecht, 2003, 485, 490 ff., Rn. 18 ff.; siehe auch jüngst die Vorlagefrage des Bundesgerichtshofs an den Europäischen Gerichtshof zur Speicherung dynamischer IP-Adressen, GRUR Praxis 2015, 38.

[27] Einen Überblick über den Streitstand gibt *Rupp*, der sich für die relative Theorie entscheidet: *Rupp*, Die grundrechtliche Schutzpflicht des Staates für das Recht auf informationelle Selbstbestimmung im Pressesektor, 2013, 98.

[28] So auch: *Redeker*, IT-Recht, [5]2012, D., Rn. 935.

[29] *Britz*, Informationelle Selbstbestimmung zwischen rechtswissenschaftlicher Grundsatzkritik und Beharren des Bundesverfassungsgerichts, in: Hoffmann-Riem (Hrsg.), Offene Rechtswissenschaft, 2010, 561, 566 ff. und *Hoffmann-Riem*, Grundrechts- und Funktionsschutz für elektronisch vernetzte Kommunikation, 134 AöR (2009), 513, 517 f.

[30] *Rössler*, Der Wert des Privaten, 2001, 205.

[31] *Rössler*, Der Wert des Privaten, 2001, 209.

Deutschland zunehmend Relevanz erfährt[32] und schließlich an die in anderen Disziplinen regelmäßig verwendete Terminologie anknüpft.

B. Preisgabe

Informationelle Preisgabe ist die langfristige Aufgabe der eigenen[33] informationellen Privatheit durch die Privatheitsträger selbst. Gegenstand der Arbeit ist nur die Preisgabe im Internetkontext, also anlässlich der Nutzung von Angeboten innerhalb des Internets als weltweitem Netzverbund.[34] Zu denken ist beispielsweise an die Preisgabe in sozialen Netzwerken, durch den Besuch datenerhebender Webseiten oder auch durch die Anwendung datenerhebender Applikationen.[35] Unerheblich ist, von welchem Endgerät die Nutzung erfolgt.

Etwas wird preisgegeben, wenn es verraten, überlassen, aufgegeben, auf es verzichtet oder es nicht mehr geheimgehalten oder nicht mehr geschützt wird.[36] Voraussetzung ist also ein irgendwie geartetes aktives Handeln, das dazu führt, dass etwas, das zunächst unter der Kontrolle der Handelnden stand, nun von Anderen kontrolliert werden kann.

Auf die Einsichts- und Urteilsfähigkeit der Preisgebenden kommt es für die Begriffsbildung nicht an. Die Preisgabe darf zwar nicht unter Bruch des Willens der Individuen erfolgen. Sie setzt jedoch nicht voraus, dass sich die Handelnden über alle Konsequenzen ihres Tuns im Klaren sind und unter sorgfältiger Abwägung aller Für und Wider eine Entscheidung treffen. Die ökonomische Irrationalität eines Entschlusses führt nicht zur Unfreiwilligkeit im Rechtssinne.[37] Vielmehr können Nutzer darauf verzichten, die Situation genau zu überdenken und aus dem Bauch heraus handeln. Sie können sich die Mühen der Wahl ersparen wollen, weil sie deren Ausgang nicht genug kümmert, als dass es den zum Verstehen der Zusammenhänge notwendigen Aufwand lohnen würde. Dieses Phänomen ist in den Wirtschaftswis-

---

[32] Beispielsweise bei *Diggelmann*, Grundrechtsschutz der Privatheit, in: Höfling (Hrsg.), Der Schutzauftrag des Rechts, 2011, 50 ff.; *Nettesheim*, Grundrechtsschutz der Privatheit, in: Höfling (Hrsg.), Der Schutzauftrag des Rechts, 2011, 7 ff. und *Schiedermair*, Der Schutz des Privaten als internationales Grundrecht, 2012.

[33] Die vorliegende Arbeit befasst sich ausschließlich mit der Preisgabe der eigene informationellen Privatheit. Man könnte auch die Bezeichnung „Selbstpreisgabe“ wählen. Nicht Gegenstand ist die Veröffentlichung von Informationen über Andere.

[34] Das World Wide Web ist nur einer von mehreren Diensten des Internets, wobei beide Begriffe in der Alltagssprache häufig synonym verwendet werden: *Hornung*, Zwei runde Geburtstage, MMR 2004, 3, 4.

[35] Zu rechtlichen und technischen Implikationen der Preisgabe in sozialen Netzwerken, siehe jüngst: *Maisch*, Informationelle Selbstbestimmung in Netzwerken, 2015.

[36] http://www.duden.de/rechtschreibung/preisgeben.

[37] Siehe unten Kapitel 7,A.VI; so auch: *Oswald*, Weicher Paternalismus und das Verbot der Teilnahme untergebrachter Personen an klinischen Arzneimittelprüfungen, in: Fateh-Moghadam/Sellmaier/Vossenkuhl (Hrsg.), Grenzen des Paternalismus, 2010, 94, 105.

senschaften unter dem Schlagwort Rationale Ignoranz geläufig. Zuerst beschrieben wurde es von *Downs*: „The amount of information it is rational for a decision-maker to acquire is determined by the following economic axiom: It is always rational to perform any act if its marginal return is larger than its marginal cost. The marginal cost of a 'bit' of information is the return foregone by devoting scarce resources – particularly time – to getting and using it. The marginal return from a 'bit' is the increase in utility income received because the information enabled the decision-maker to improve his decision."[38] Sobald der Aufwand, der benötigt wird, um alle relevanten Zusammenhänge zu verstehen, größer ist als der daraus folgende Nutzen, ist Ignoranz rational.

Nutzer können unvernünftige, gefährliche und inkonsequente Entscheidungen fällen, die sie bei reiflicher Überlegung wohl so nie getroffen hätten. Auch können sie trotz sorgfältiger Abwägung bestimmte – ihnen unbekannte oder entfallene – Fakten nicht mit einbeziehen und daher für sie ungünstige Entscheidungen treffen. Solche Prozesse können bewusst oder unbewusst erfolgen.

Keine Preisgabe liegt jedoch vor, wenn den Nutzern etwas rechtswidrig oder aufgrund gesetzlicher Grundlage ohne eigenes Zutun genommen wird, da es dann gerade nicht auf den Akt der Preisgabe durch die Nutzer ankommt. Beispiele für die nicht als Preisgabe zu bezeichnende Datenerhebung auf gesetzlicher Grundlage sind demnach gesetzlich erlaubte Datenerhebungen durch den Staat.

Abstraktes Objekt der Preisgabe ist die informationelle Privatheit. Konkret geben die Einzelnen sie langfristig auf, indem sie Daten über sich selbst preisgeben. Diese Daten befähigen Dritte dazu, durch Verarbeitung und Nutzung der Daten Informationen über die Privatheitsträger zu generieren.[39] Erst das Entstehen solcher Informationen bei Dritten führt dazu, dass dort ein Wissen über Angelegenheiten vorhanden ist, die ursprünglich der informationellen Privatheit der Privatheitsträger zuzurechnen waren. Welche Informationen Dritte aus bei ihnen vorhandenen personenbezogenen Daten gewinnen, können die Individuen nicht kontrollieren. Wohl können sie aber die Preisgabe ihrer Daten als notwendigen Schritt zur Entstehung der Informationen beherrschen. Wenn abstrakt von der Preisgabe informationeller Privatheit gesprochen wird, entspricht dies daher konkret der Preisgabe von personenbezogenen Daten.

Im Internetkontext kann die Preisgabe auf eine unüberschaubare Vielzahl an Arten und Weisen explizit (siehe I) oder implizit geschehen (siehe II).

I. Explizite Preisgabe

Zunächst zu denken ist an eine explizite Preisgabe, bei der die Nutzer aktiv am Preisgabeprozess beteiligt sind. Beispiele sind die Erstellung und Unterhaltung von

[38] *Downs*, An Economic Theory of Political Action in a Democracy, 65 J. of Political Economy (1957), 135, 146.

[39] Zur Unterscheidung zwischen Daten und Informationen, siehe oben Kapitel 2,A.III.

Profilen in sozialen Netzwerken in all ihren Formen, inklusive dem Hochladen vielfältiger Fotos. Gleiches gilt für Internet-Tagebücher, Foren, persönliche Webseiten, das Veröffentlichen von Webcam-Aufnahmen[40] und das Online-Stellen von Protokollen der eigenen Aktivitäten (sogenannte Lifelogs).[41]

Die genannten Formen der Privatheitsaufgaben haben gemein, dass sie bewusst und zielgerichtet erfolgen. Die Nutzer wollen ihre informationelle Privatheit partiell aufgeben und damit ihnen bekannte oder unbekannte Adressaten erreichen. Die Rede ist vom „Datenexhibitionismus"[42] der Nutzer, der kombiniert wird mit einem gesellschaftlichen Hang zum Voyeurismus. Weiter sind diese Ausprägungen der Privatheitsaufgabe dadurch gekennzeichnet, dass die Nutzer sie vermeintlich kontrollieren können. Das bewusste Handeln hat zur Folge, dass häufig die Illusion entsteht zu wissen, welche personenbezogenen Daten preisgeben werden. Zudem ist die Preisgabe dieser Daten meist auf die Wahrnehmung durch natürliche Personen gerichtet, die regelmäßig ein persönliches Interesse an der Kenntnisnahme haben.

II. Implizite Preisgabe

Zur Preisgabe zählen auch Verhaltensweisen, die sich als implizite, technisch im Hintergrund erfolgende Preisgabe qualifizieren lassen. Die implizite Preisgabe erfolgt, anders als die explizite, nicht zielgerichtet, sondern als Nebenprodukt der Internetnutzung. Die Nutzer sind im Falle solcher beiläufiger Preisgabe „nicht aktiv und/oder bewusst am Prozess der Datengenerierung und Speicherung beteiligt", vielmehr werden die Daten „– oftmals ohne Wissen des Nutzers – im Hintergrund erfasst".[43] Der aktive Beitrag der Nutzer beschränkt sich damit häufig auf die willentliche Nutzung internetbasierter Angebote und Anwendungen, in deren Zusammenhang die Datenerhebung erfolgt. Insbesondere im Wege weitreichender vorformulierter Einwilligungserklärungen lassen sich Anbieter Zugriffsrechte auf zahlreiche Systemfunktionen gewähren, wie sich am Beispiel diverser Smartphone-Apps zeigt.

Das Bundesverfassungsgericht führt zum Entstehen impliziter Informationen in seiner Entscheidung zu den Online-Durchsuchungen aus: „Im Rahmen des Datenverarbeitungsprozesses erzeugen informationstechnische Systeme zudem selbsttätig zahlreiche weitere Daten, die ebenso wie die vom Nutzer gespeicherten Daten im Hinblick auf sein Verhalten und seine Eigenschaften ausgewertet werden können. In

---

[40] Jedoch bleibt bislang die allgemein zugängliche Übertragung privater Räume per Webcam auf Einzelfälle beschränkt, wie beispielsweise auf die inzwischen offline gestellte Webseite http://www.jennicam.org/, auf der das Alltagsleben der Betroffenen mit ihrem Einverständnis live im Internet wiedergegeben wurde. Die Übertragung privater Räume ist entgegen anderslautender Bedenken nicht automatische Konsequenz des Besitzes einer Webcam, so aber wohl: *Rössler*, Der Wert des Privaten, in: Jurczyk (Hrsg.), Das Private neu denken, 2008, 282, 289.

[41] Zur moralischen Bewertung und möglichen rechtlichen Rahmenbedingungen von Lifelogs: *Allen*, Dredging up the Past, 75 Chicago L. Rev. (2008), 47, 47 ff.

[42] *Baum*, Unerledigte Verfassungsaufträge, DuD 2011, 595.

[43] *Klein/Leithold/Zell u. a.*, Digitale Profilbildung und Gefahren für die Verbraucher, 2010, 5.

der Folge können sich im Arbeitsspeicher und auf den Speichermedien solcher Systeme eine Vielzahl von Daten mit Bezug zu den persönlichen Verhältnissen, den sozialen Kontakten und den ausgeübten Tätigkeiten des Nutzers finden. Werden diese Daten von Dritten erhoben und ausgewertet, so kann dies weitreichende Rückschlüsse auf die Persönlichkeit des Nutzers bis hin zu einer Profilbildung ermöglichen".[44] Gerade aus diesem neuen Bedrohungspotenzial ergab sich das Bedürfnis zur Entwicklung des Grundrechts auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme (sogenanntes IT-Grundrecht, Art. 2 Abs. 1 in Verbindung mit Art. 1 Abs. 1 GG).[45]

Die erhobenen Daten können auf vielfältige Weise genutzt werden:

Suchmaschinen- und E-Commerce-Angebote werden im Regelfall personalisiert dargeboten, das heißt, sie sollen den Nutzern das richtige Angebot zur richtigen Zeit liefern. Dies geschieht sowohl durch Produktvorschläge (seien es personalisierte Suchmaschinentreffer oder Kaufvorschläge im Online-Shop) als auch durch sogenanntes Targeted Advertising. Berühmtes (Offline-) Beispiel für Targeted Advertising lieferte die US-Kaufhauskette Target, die anhand des Einkaufsverhaltens ihrer Kundinnen auf das Vorliegen einer Schwangerschaft schließen und mit entsprechenden Offerten reagieren konnte, teilweise bevor die Kundinnen selbst von ihrer Schwangerschaft wussten.[46]

Voraussetzung für das Entstehen personalisierter Angebote ist die vorherige Speicherung, Zusammenführung und Weiterleitung von Vorlieben sowie Browse- und Kaufverhalten.[47] Ähnlich sind soziale Netzwerke bemüht, den Nutzern ein auf sie zugeschnittenes Angebot zu bieten, beispielsweise im Rahmen von Kontaktvorschlägen oder dem Hervorheben von potenziell interessierenden Einträgen oder kommerziellen Angeboten.

Um den Nutzern personalisierte Angebote liefern zu können, muss im Rahmen des sogenannten Trackings ein Überblick über ihr vorheriges Verhalten gewonnen werden. Dafür ist dieses bestimmten Usern zuzuordnen. Einer namentlichen Benennung bedarf es nicht, vielmehr ist es relevant zu wissen, dass es sich um die identischen User handelt und welche Vorlieben sie pflegen. Das Tracking erfolgt insbesondere durch das Speichern von IP-Adressen, das Setzen von Cookies sowie das Verwenden von Web-Bugs, Browser- und OS-Fingerprints.[48] Unter dem Begriff Web-Bug versteht man ein transparentes, für die Nutzer nicht sichtbares Bild in der Größe eines Pixels, das von Webseitenanbietern als Link zu einem dritten Server in die Webseiten integriert wird. Beim Aufrufen einer Webseite folgt der Browser au-

---

[44] BVerfGE 120, 274 (305).

[45] BVerfGE 120, 274.

[46] *Duhigg*, How Companies Learn Your Secrets, 16.02.2012.

[47] Zur Funktionsweise personalisierter Suchmaschinen: *van Hoboken*, Search engine freedom 2012, 291 ff.

[48] Die Electronic Frontier Foundation stellt Nutzern ein Instrument zur Verfügung, um die Identifizierbarkeit ihrer Computer mithilfe ihrer Fingerabdrücke feststellen zu können: https://panopticlick.eff.org/.

tomatisch dem Link zu der dritten Webseite. Die dritte Webseite kann so Cookies im Browser setzen und zudem die Information abspeichern, von welcher Webseite der Browser das Web-Bug erhalten hat. Indem Web-Bugs auf einer Vielzahl von Webseiten angebracht werden, können vielfältige Informationen gewonnen und verkauft werden.[49] Entsprechend funktionieren auch die sogenannten Like-Buttons und Werbebanner, die ein Tracking des Nutzerverhaltens ermöglichen. Als Browser-/OS-Fingerprinting werden alle Datenverarbeitungsvorgänge bezeichnet, bei denen die standardisiert vom Browser beziehungsweise dem Betriebssystem übermittelten Informationen erhoben, gespeichert und ausgewertet werden.[50]

Diese nun einzelnen Nutzern zugeordneten Daten aus verschiedenen Quellen werden bei den Anbietern selbst sowie dritten Stellen gesammelt. Beispiel für Letztere sind weltweit agierende Firmen wie BlueKai[51] oder Acxiom,[52] die detaillierte Datensätze über viele Millionen Menschen pflegen und anderen Firmen anbieten.

Diese Daten können durch Datenanalyse (sogenanntes Data Mining) ausgewertet werden. Dies geschieht, indem von den Nutzern erhobene Daten auf einen vorbereiteten Datenbestand angewendet werden, um durch datenverarbeitungsgestützte Algorithmen verborgene Zusammenhänge und Tendenzen aufzudecken.[53] Das viel zitierte Schlagwort Big Data bedeutet wörtlich übersetzt soviel wie große Datenmengen. Das Ziel deren Analyse ist es, „die stetig zunehmenden Datenmengen analytisch miteinander zu verknüpfen, um daraus ökonomische, soziale oder wissenschaftliche Erkenntnisse zu gewinnen".[54] Die Auswertung von Big Data beruht auf dem Konzept, ausreichende Details aus der Vergangenheit zu sammeln, sie mit den richtigen analytischen Werkzeugen zu untersuchen und dadurch unerwartete Verbindungen und Zusammenhänge herzustellen, die im Regelfall präzise Vorhersagen zulassen. Diese Datenuntersuchung wird dadurch ermöglicht, dass eine unüberschaubare Anzahl an Menschen große Teile ihres Alltags mithilfe von Internetanwendungen bewältigt. Zurecht wird jedoch darauf hingewiesen, dass sich die Analyse von Big Data auf Daten derjenigen beschränkt, die Zugang zum Internet haben und dieses in signifikantem Umfang nutzen. In dem Maße, in dem politische und wirtschaftliche Entscheidungen verstärkt auf Grundlage von Big-Data-Analysen getroffen werden, bleibt der Teil der Weltbevölkerung, der entsprechende Daten

---

[49] *Grimm*, Spuren im Netz, DuD 2012, 88, 89 f.

[50] Vgl.: *Zeidler/Brüggemann*, Die Zukunft personalisierter Werbung im Internet, CR 2014, 248, 252.

[51] http://www.bluekai.com/.

[52] http://acxiom.com/.

[53] *Bensberg*, Die technischen Potenziale analytischer Informationssysteme, in: Redeker/Hoppen (Hrsg.), DGRI Jahrbuch 2011, 2012, 181, 186 f. und *Scholz*, Datenschutz bei Data Warehousing und Data Mining, in: Roßnagel (Hrsg.), Handbuch Datenschutzrecht, 2003, 1833, 1837, Rn. 3, 1843 ff., Rn. 27 ff.

[54] *Ohrtmann/Schwiering*, Big Data und Datenschutz, NJW 2014, 2984; dort auch zu rechtlichen Problematiken im Zusammenhang mit der Big Data-Analyse; weiterführend: *Roßnagel*, Big Data – Small Privacy?, ZD 2013, 562 ff.

nicht produziert, außer Betracht.[55] Anders als bei herkömmlichen Vorhersageverfahren (die Rede ist auch von der „small-data world“) bedarf es im Rahmen der Big-Data-Analyse keiner Ausgangshypothese, das Verständnis der zugrunde liegenden Kausalitäten ist irrelevant, einzig entscheidend ist das Bestehen von Zusammenhängen.[56]

So können neue Informationen erzeugt und Vorhersagen über zukünftige Vorlieben und zukünftiges Verhalten getroffen werden (sogenanntes Profiling).[57] Dafür werden die Nutzer anhand der abgerufenen Ressourcen in charakteristische Besuchergruppen eingeteilt und ihnen sodann spezifische, auf ihre angenommenen Interessen zugeschnittene Inhalte präsentiert.[58] Die so entdeckten Korrelationen sind den Nutzern regelmäßig selbst vorher nicht bekannt, das System sucht vielmehr autonom nach Mustern und generiert neue Wissenszusammenhänge.[59] Die Bandbreite der technischen Möglichkeiten ist dabei sehr groß: Anhand ihrer Profile lässt sich beispielsweise häufig eine Vorhersage darüber treffen, welchen Preis die Nutzer für ein bestimmtes Produkt bezahlen würden. Entsprechend kann der Preis nutzerindividuell angepasst werden.[60]

Die Erstellung von Nutzerprofilen ist nach deutschem Recht nicht allgemein, sondern nur für die Nutzungsdaten bei Telemedien geregelt. Hier ist sie, soweit keine Einwilligung vorliegt, nur nach Maßgabe des § 15 Abs. 3 TMG zulässig.[61] Demnach dürfen Diensteanbieter aus selbst erhobenen Daten für die Zwecke der Werbung, der Marktforschung oder zur bedarfsgerechten Gestaltung der Telemedien (also insbesondere zum Anfertigen personalisierter Angebote)[62] pseudonyme Nutzerprofile erstellen, soweit die Nutzer nicht widersprechen.

---

[55] *Lerman*, Big Data and its Exclusions, 66 Stanford L. Rev. Online (2013), 55 ff.

[56] *Mayer-Schönberger/Cukier*, Big Data, 2013, 61, 4.

[57] Zum technischen Ablauf: *Kelbert/meh Shirazi/Simo u. a.*, State of Online Privacy, in: Buchmann (Hrsg.), Internet Privacy, 2012, 189, 233 ff. und *Schnabel*, Datenschutz bei profilbasierten Location Based Services, 2009, 180 ff., der auch ausführlich die verfassungs- und datenschutzrechtliche Zulässigkeit der Profilbildung analysiert.

[58] *Bensberg*, Die technischen Potenziale analytischer Informationssysteme, in: Redeker/Hoppen (Hrsg.), DGRI Jahrbuch 2011, 2012, 181, 193 f.

[59] *Scholz*, Datenschutz bei Data Warehousing und Data Mining, in: Roßnagel (Hrsg.), Handbuch Datenschutzrecht, 2003, 1833, 1844, Rn. 28 f.; einen Einblick in mögliche Erkenntnisse gibt: *Welchering*, Vom überwachten Bürger zum gläsernen Menschen, DANA 2014, 144 ff.

[60] *Newman* analysiert diese sogenannte Preis-Diskriminierung und liefert empirische Nachweise: *Newman*, The Costs of Lost Privacy, 40 William Mitchell L. Rev. (2014), 849, 865 ff. Beispielsweise zeigte sich, dass Mac-Nutzer durchschnittlich teurere Hotels buchen als PC-Nutzer, woraufhin die Urlaubs-Suchmaschine Orbitz die priorisiert angezeigten Angebote danach sortierte, mit welchem Gerät die Nutzer die Webseite aufriefen, *Mattioli*, On Orbitz, Mac Users Steered to Pricier Hotels, 6.6.2012.

[61] *Spindler/Nink*, in: Spindler/Schuster (Hrsg.), Recht der elektronischen Medien, 2015, § 15 TMG, Rn. 8.

[62] *Spindler/Nink*, in: Spindler/Schuster (Hrsg.), Recht der elektronischen Medien, 2015, § 15 TMG, Rn. 7 f.

Entscheidungen, die für die Betroffenen eine rechtliche Folge nach sich ziehen oder sie erheblich beeinträchtigen, dürfen in Deutschland grundsätzlich nicht ausschließlich auf eine automatisierte Verarbeitung personenbezogener Daten gestützt werden (§ 6a BDSG).[63]

Unklarheit besteht hingegen hinsichtlich des Umgangs mit Cookies. Nach der sogenannten EU-Cookie-Richtlinie[64] bedarf das Setzen von Cookies der ausdrücklichen Zustimmung der Nutzer, also eines Opt-ins. Erwägungsgrund 66 der Richtlinie relativiert dies jedoch, wenn dort davon ausgegangen wird, die Einwilligung könne auch durch die Handhabung der entsprechenden Einstellungen des Browsers erfolgen. Trotz abgelaufener Umsetzungsfrist hat Deutschland kein Erfordernis eines ausdrücklichen Opt-ins gesetzlich geregelt. Es wäre daher davon auszugehen, dass der Richtlinie nun unmittelbare Wirkung zukommt. Da das Europarecht keine horizontale direkte Anwendbarkeit von Richtlinien kennt,[65] würde die unmittelbare Wirkung allerdings nur im Staat-Bürger-Verhältnis gelten, nicht im regelmäßig viel relevanteren Verhältnis Privater untereinander. In einer Stellungnahme hat die EU-Kommission jedoch jüngst bestätigt, dass Deutschland die Richtlinie bereits ordnungsgemäß umgesetzt hat.[66] Dies vermag zu verwundern, da sich mit dieser Einschätzung ein Erwägungsgrund gegenüber dem umsetzungspflichtigen Richtlinien-Wortlaut durchsetzt.

In den Vereinigten Staaten hingegen ist zur Durchführung der beschriebenen Praktiken generell keine Zustimmung der Nutzer erforderlich.

Unabhängig von der rechtlichen Bewertung im Einzelnen wird jedenfalls deutlich, dass sowohl explizit als auch implizit große Mengen personenbezogener Daten im Internet preisgegeben werden. Dabei fehlt es häufig an Transparenz, sodass Nutzer nicht übersehen können, wie explizit preisgegebene Daten – etwa besonders sensible Daten aus sozialen Netzwerken – im weiteren Verlauf verwendet werden beziehungsweise welche implizit preisgegebenen Daten überhaupt erhoben werden.

Die bislang gefundenen Erkenntnisse lassen sich wie folgt zusammenfassen: Informationelle Preisgabe ist die langfristige Aufgabe der eigenen informationellen Privatheit durch die Privatheitsträger selbst. Gegenstand der Arbeit ist nur die informationelle Preisgabe im Internetkontext.

Informationelle Privatheit ist ein Aspekt der Privatheit. Privatheit dient der Sicherung der individuellen Autonomie und erfasst alles, was ihre Träger aus beliebigen Gründen nicht zeigen möchten. Die Unterkategorie informationelle Privatheit wird verstanden als die Möglichkeit der Einzelnen, selbst über die Preisgabe und Verwendung der eigenen personenbezogenen Daten zu bestimmen.

---

[63] Zu den zugrunde liegenden Überlegungen: *Mayer-Schönberger/Cukier*, Big Data, 2013, 176 f.

[64] RL 2009/136/EG v. 25.11.2009; die Diskussion nachzeichnend: *Zeidler/Brüggemann*, Die Zukunft personalisierter Werbung im Internet, CR 2014, 248, 251.

[65] EuGH NJW 1994, 2473, 2474 (Faccini Dori v. Recreb Srl).

[66] *Schneider*, EU-Kommission: Cookie-Richtlinie ist in Deutschland umgesetzt, 5.2.2014.

Die Preisgabe informationeller Privatheit ist ein im weitesten Sinne aktives Handeln der Privatheitsträger, mit dem sie langfristig die Kontrolle über ihre personenbezogenen Daten aufgeben. Notwendig ist nicht, dass die Nutzer gezielt ihre Daten preisgeben, vielmehr kommt es darauf an, ob sie einen Beitrag zur Datenerhebung leisten, der staatlicherseits verhindert werden kann. Gesetzlich autorisierte sowie von vornherein rechtswidrige Datenerhebungen sind nicht erfasst, da sie unabhängig vom Willen der Nutzer erfolgen. Auf die Rationalität der Preisgabe kommt es nicht an. Die Preisgabe kann explizit oder implizit erfolgen. Unter expliziter Preisgabe ist eine bewusste und zielgerichtete Preisgabe zu verstehen. Zudem kann die Preisgabe implizit erfolgen, also anlässlich der Nutzung von Internetangeboten und ohne intentionales Zutun der Preisgebenden.

Kapitel 3

Gefährdete Rechtsgüter

Bei der Untersuchung einer staatlichen Pflicht wie auch einer staatlichen Befugnis zur Verhinderung informationeller Preisgabe im Internet ist danach zu differenzieren, welches Gut hierdurch primär[1] geschützt werden soll. Zu diesem Zweck ist zu untersuchen, welche tatsächlichen Gefahren durch informationelle Preisgabe im Internet drohen (siehe A) und welchen Stellenwert die deutsche und die US-amerikanische Verfassung jeweils den durch die informationelle Preisgabe bedrohten Rechtsgütern zumisst (siehe B und C). Anschließend wird ein Vergleich zwischen den Stellenwerten der bedrohten Rechtsgüter in Deutschland und den Vereinigten Staaten gezogen (siehe D).

A. Faktische Gefahren informationeller Preisgabe im Internet

Grundlage für die Bestimmung der gebotenen rechtlichen Schritte ist die Analyse der tatsächlichen Gefahren informationeller Preisgabe. Die Konsequenzen der Preisgabe informationeller Privatheit können dabei auf dem Bekanntsein explizit preisgegebener personenbezogener Daten beruhen sowie auf der Analyse der implizit preisgegebenen Daten.

Zum Verständnis der tatsächlichen Gefahren informationeller Preisgabe lohnt ein Blick auf die aktuelle US-amerikanische Diskussion. Dort besteht ein im internationalen Vergleich geringes Niveau des Privatheitsschutzes der Bürger. Durch – oftmals plakative – Darlegung des Bedrohungspotenzials, das dem Verlust informationeller Privatheit zukommt, werden in den USA die rechtspolitischen Forderungen nach Erhöhung des Privatheitsschutzes untermauert.

Im Folgenden werden, ausgehend von einer Entkräftung des viel zitierten „Ich-habe-nichts-zu-verbergen"-Arguments (siehe I), die faktischen Gefahren analysiert, die informationelle Preisgabe für die Preisgebenden selbst (siehe II) und für Allgemeinwohlbelange (siehe III) bergen kann.

---

[1] Zur Frage, wie der Hauptzweck der staatlichen Intervention zu bestimmen ist: siehe unten Kapitel 7,B.II.

I. Der „Ich-habe-nichts-zu-verbergen“-Fehlschluss

„TRAPS: Was soll ich denn für ein Verbrechen begangen haben?

STAATSANWALT: Ein unwichtiger Punkt, mein Freund. Ein Verbrechen läßt sich immer finden.“[2]

Mit diesen Worten beginnt das fiktive Gerichtsverfahren, in dem die Akteure in *Dürrenmatts* Hörspiel „Die Panne“ einen ahnungslosen Reisenden schließlich davon überzeugen, einen Mord begangen zu haben und ihn zur Todesstrafe verurteilen. Ausgangspunkt der Verurteilung ist die Leichtsinnigkeit des Reisenden *Traps*, der Daten über sich preisgibt, ohne zu realisieren, dass diese, aus dem Kontext gerissen, seinen Untergang bedeuten können.

„TRAPS: Kein Bange, mein lieber Herr Verteidiger, wenn erst einmal das Verhör beginnt, werde ich auf der Hut sein.

VERTEIDIGER: Unglücksmensch, was meinten Sie damit: wenn einmal erst das Verhör beginnt?

TRAPS: Nun? Hat es etwa schon begonnen?“[3]

Das Stück aus dem Jahr 1961 greift einen der auch heute noch gängigsten Mythen im Bereich Privatheit auf: Insbesondere zur Rechtfertigung staatlicher Eingriffe in die informationelle Privatheit der Bürger wird vorgetragen, wer nichts zu verbergen habe, müsse durch Überwachung auch nichts befürchten.[4]

Diese Behauptung beruht bereits auf der unzutreffenden Annahme, Privatheit bezwecke das Verstecken von Schlechtem.[5] Privatheit schützt vielmehr alles, was ihre Träger aus beliebigen Gründen nicht zeigen möchten.[6]

Das „Ich-habe-nichts-zu-verbergen“-Argument trägt zudem auch argumentativ nicht, wie sich sowohl am Beispiel an sich nicht kompromittierender personenbezogener Daten als auch anhand von Wissen über tatsächlich belastendes Verhalten zeigt.

Zunächst ist an einzelne personenbezogene Daten zu denken, die an sich nicht fehlerhaftes Vorgehen dokumentieren. Nutzer mögen gewillt sein, diese personenbezogenen Daten separat preiszugeben, da von ihnen kein Unheil zu drohen scheint. Doch die Situation kann sich in ihr Gegenteil verkehren, sobald die personenbezogenen Daten aus dem Kontext gerissen und anderweitig verbunden und analysiert

---

[2] *Dürrenmatt*, Die Panne, 1985 (Original: 1961), 17.

[3] *Dürrenmatt*, Die Panne, 1985 (Original: 1961), 24 f.

[4] Dazu auch *Soloves* einflussreicher Aufsatz: *Solove*, “I’ve Got Nothing to Hide” and Other Misunderstandings of Privacy, 44 San Diego L. Rev. (2007), 745 ff.

[5] So auch: *Solove*, Nothing to Hide, 2011, 26; vgl.: *Schulhofer*, More Essential Than Ever, 2012, 171.

[6] Siehe oben Kapitel 2,A.

werden.[7] So können aus an sich nicht kompromittierenden personenbezogenen Einzeldaten Informationen gewonnen werden, die die Nutzer lieber verborgen hätten.[8] Als Beispiel zu nennen sind Informationen über politische Präferenzen der Nutzer und ihres Umfelds, die aus der Analyse von Freundschaften in sozialen Netzwerken gewonnen werden können.[9] Auch kann aus der Untersuchung von Facebook-Freundschaften mit hoher Treffsicherheit auf eine, je nach gesellschaftlichem Umfeld vielleicht lieber nicht offengelegte, homosexuelle Orientierung der jeweiligen Nutzer geschlossen werden.[10] Für gesellschaftliches Aufsehen sorgte das 2012 bekannt gewordene und alsbald unter öffentlichem Druck aufgegebene Vorhaben der Schutzgemeinschaft für allgemeine Kreditsicherung (SCHUFA) und des Hasso-Plattner-Instituts, soziale Netzwerke als Quelle zur Beurteilung der Kreditwürdigkeit der Nutzer heranzuziehen.[11]

Bedenkt man, dass die Nutzer keine Möglichkeit haben, abzuschätzen, welche Informationen durch Dritte im Rahmen von Datenanalyse erzielt werden können, erscheint es schwer auszuschließen, dass dabei Erkenntnisse zutage treten, die sie lieber nicht offengelegt hätten.[12] Ähnliches gilt für Diskriminierungsmöglichkeiten, die dadurch entstehen, dass aus der Verbindung bestimmter an sich harmloser personenbezogener Daten sensible Informationen erlangt werden.

Der Gedanke lässt sich zudem ausdehnen auf Vorkommnisse, die sowohl auf soziale als gegebenenfalls auch auf rechtliche Weise missbilligenswert sind.[13] Menschen begehen Fehler. Gravierendes Fehlverhalten wird sowohl sozial als auch rechtlich geahndet, wenn es bekannt wird. Führt allerdings jeder noch so kleine Makel zu sozialer und rechtlicher Sanktion, wird eine durchgehende Angst vor Missgeschicken gefördert. Daher ist es in der Gesellschaftsordnung auch üblich, dass kleinere menschliche Fehltritte ungesühnt bleiben können. Sie können zwischenmenschlich verziehen werden, strafprozessrechtlich ist an die Möglichkeit der Verfahrensbeendigung nach §§ 153, 154 StPO zu denken. Nutzer können ein anerkennenswertes Interesse daran haben, dass das Wissen über diskreditierende Umstände jedenfalls nicht dauerhaft und nicht auf einfachem Wege verfügbar ist. Ein solches Recht auf Vergessenwerden kann, jedenfalls nach europäischem Recht,

---

[7] Dies hat das Bundesverfassungsgericht bereits im Volkszählungsurteil erkannt, wenn es ausführt, unter den Bedingungen der automatischen Datenverarbeitung gäbe es kein belangloses Datum mehr, BVerfGE 65, 1 (45).

[8] So auch: *Solove*, "I've Got Nothing to Hide" and Other Misunderstandings of Privacy, 44 San Diego L. Rev. (2007), 745, 769.

[9] *Hartzog/Selinger*, Obscurity, 17.1.2013.

[10] *Jernigan/Mistree*, Gaydar: Facebook friendships expose sexual orientation, 14 First Monday (2009).

[11] *Wilkens*, Bericht: Schufa will Daten in sozialen Netzwerken nutzen, 7.6.2012. Dieses Vorgehen scheint international jedoch nicht unüblich: *Lobosco*, Facebook friends could change your credit score, 27.8.2013.

[12] So auch: *Solove*, "I've Got Nothing to Hide" and Other Misunderstandings of Privacy, 44 San Diego L. Rev. (2007), 745, 766.

[13] *Bull*, Informationelle Selbstbestimmung, 2009, 43 f.

auch hinsichtlich an sich wahrer Berichterstattung und Zusammenführung von Informationen bestehen. Dies gilt insbesondere hinsichtlich der Angebote von Suchmaschinen, da diese es allen Internetnutzern ermöglichen, auf einfache Weise einen strukturierten Überblick über Informationen zu einer Person zu erhalten, die potenziell zahlreiche Aspekte von deren Privatleben betreffen und ohne die betreffende Suchmaschine nicht oder nur sehr schwer hätten miteinander verknüpft werden können.[14] Hier ist nach der Entscheidung des Europäischen Gerichtshofs in Sachen Google v. Costeja González ein Ausgleich zwischen den Interessen der Suchmaschinenbetreiber und den Persönlichkeitsrechten der Betroffenen zu finden, wobei regelmäßig die Persönlichkeitsrechte überwiegen.[15]

Häufig haben Nutzer also ein Interesse daran, dass sowohl unbedenkliche, aber kontextbezogen trotzdem unangenehme, als auch bedenkliche Daten nicht preisgegeben werden oder nicht dauerhaft bekannt bleiben. Das „Ich-habe-nichts-zu-verbergen"-Argument trägt somit in doppelter Hinsicht nicht.

II. Gefahren für die Preisgebenden

Informationelle Preisgabe kann zu einer Vielzahl von Gefahren für die Preisgebenden führen, wenn es zu einem direkten Missbrauch der entsprechenden Daten kommt. Zu denken ist beispielsweise an finanzielle Nachteile durch Diskriminierung bei der Kreditvergabe, wenn eine Datenanalyse auf eine geringe Bonität der jeweiligen Nutzer schließen lässt oder durch Preis-Diskriminierung, wenn identische Produkte unterschiedlichen Nutzern jeweils zu dem Preis angeboten werden, den die jeweiligen Nutzer – ausgehend von der Analyse ihrer zuvor preisgegebenen Daten – vermutlich zu zahlen bereit sind.

Auf der Hand liegen auch Risiken, die dadurch entstehen, dass (zukünftigen) Arbeitgebern Informationen zugänglich sind, die sie besser nicht erreicht hätten, beispielsweise unangenehme Fotos aus der Vergangenheit der Bewerber/Arbeitnehmer oder abschätzige Äußerungen in Statusmeldungen in sozialen Netzwerken. In drastischen Fällen kann informationelle Preisgabe sogar zu lebensbedrohlichen Folgen führen, etwa, wenn ein potenzieller Mörder auf diese Weise den Aufenthaltsort des Opfers erfährt.

Aufgrund der Vielschichtigkeit aller unter Umständen mit informationeller Preisgabe in Verbindung zu bringender Gefahren ist eine abschließende Erörterung weder möglich noch zweckdienlich. Während die Einordnung dieser direkten Gefahren bereits Gegenstand einer Vielzahl von Untersuchungen war,[16] soll im Folgenden

[14] EuGH EuZW 2014, 541 (546).

[15] EuGH EuZW 2014, 541 (547).

[16] Zu Nachteilen bei der Kreditvergabe: *Wilkens*, Bericht: Schufa will Daten in sozialen Netzwerken nutzen, 7.6.2012; zur Preisdiskriminierung: *Newman*, The Costs of Lost Privacy, 40 William Mitchell L. Rev. (2014), 849 ff.; zum Interesse von Arbeitnehmern an den öffentlich verfügbaren Informationen über Bewerbern: *Redaktion FD-ArbR*, Jedes zweite Unternehmen überprüft Bewerber in Sozialen Netzwerken, FD-ArbR 2015, 369739 ff.; zur Veröffentlichung abschätziger

der Fokus daher auf den indirekten Gefahren informationeller Preisgabe liegen. Die genannten und viele andere offensichtliche Gefahren können dazu führen, dass sich das Preisgabeverhalten der Nutzer insgesamt ändert, wie die folgenden Ausführungen zeigen werden.

Die automatisierte Verarbeitung personenbezogener Daten könnte in ihren Wirkungen mit konventioneller Überwachung vergleichbar sein und Auswirkungen auf den individuellen Erkenntnisprozess haben. Dieser wird in Anlehnung an *Steinmüller* definiert als „Prozeß der Erzeugung handlungsrelevanter ideeller Modelle in einem Empfänger über Originale, wobei letztere beliebige Originale der Innen- und Außenwelt sein können“.[17]

Elektronische Aufzeichnungen über intellektuelle Aktivitäten könnten diesen Erkenntnisprozess beeinträchtigen, wenn eine neutrale Quellenauswahl erschwert (siehe 1.) und die Preisgebenden der Selbstzensur ausgesetzt werden (siehe 2.).

1. Beeinträchtigung neutraler Quellenauswahl

Zunächst könnte informationelle Preisgabe mittelbar eine neutrale Quellenauswahl stören.

Der intellektuelle Erkenntnisprozess findet auf Grundlage der zur Erforschung des Sachverhalts zur Verfügung stehenden Quellen statt. Er beinhaltet die Konfrontation mit von Anderen entwickelten Ideen zum Zweck ihrer Bewertung, Verbesserung oder Übernahme. Das Aufdrängen vorgefertigter Meinungen kann die erzielten Erkenntnisinhalte beeinflussen.

Die Erkundung der die Einzelnen interessierenden Fragen findet heute zu einem beträchtlichen Teil durch Internetrecherche statt. Der Bundesgerichtshof führt dazu aus: „Das Internet stellt weltweit umfassende Informationen in Form von Text-, Bild-, Video- und Audiodateien zur Verfügung. Dabei werden thematisch nahezu alle Bereiche abgedeckt und verschiedenste qualitative Ansprüche befriedigt. So sind etwa Dateien mit leichter Unterhaltung ebenso abrufbar wie Informationen zu Alltagsfragen bis hin zu hochwissenschaftlichen Themen. Dabei ersetzt das Internet wegen der leichten Verfügbarkeit der Informationen immer mehr andere Medien, wie zum Beispiel Lexika, Zeitschriften oder Fernsehen. Darüber hinaus ermöglicht es den weltweiten Austausch zwischen seinen Nutzern, etwa über E-Mails, Foren, Blogs und soziale Netzwerke.“[18]

Äußerungen in sozialen Netzwerken: *Bauer/Günther*, Kündigung wegen beleidigender Äußerungen auf Facebook. NZA 2013, 67 ff.; zur Veröffentlichung von Fotos, die im Zusammenhang mit der Arbeit stehen: *Klinkhammer/Müllejans*, Veröffentlichen von Fotos in sozialen Netzwerken, ArbRAktuell 2014, 503 ff.

[17] *Steinmüller* verwendet die Bezeichnung „Informationsprozeß“ anstelle von „Erkenntnisprozess“: *Steinmüller*, Informationsrecht und Informationspolitik, in: ders. (Hrsg.), Informationsrecht und Informationspolitik, 1976, 1, 7.

[18] BGHZ 196, 101 (109). Einen umfassenden empirischen Überblick über die Bedeutung des Internets für den Zugang zu Nachrichten liefert *Reuters Institute for the Study of Journalism*, Reuters Institute Digital News Report 2014, 2014.

Nach einer BITKOM-Umfrage informierten sich 2013 in Deutschland 38 Prozent der Internetnutzer in sozialen Netzwerken über das Tagesgeschehen.[19] In einer Studie des Pew Research Center im Jahr 2010 in den USA gaben 34 Prozent der Befragten an, am Vortrag Nachrichten online konsumiert zu haben, 17 Prozent hatten am Vortag ein Online-Nachrichtenmagazin gelesen.[20] 47 Prozent nutzten Suchmaschinen mindestens einmal die Woche zur Versorgung mit Nachrichten, 17 Prozent sogar täglich.[21] 16 Prozent versorgten sich regelmäßig, 26 Prozent manchmal über soziale Netzwerke mit Nachrichten (bei den 30–49-Jährigen liegen die Zahlen sogar bei 19 und 27 Prozent); Blogs wurden von elf Prozent regelmäßig, von 24 Prozent manchmal zur Versorgung mit Nachrichten genutzt.[22]

Bei der Online-Versorgung mit Nachrichten können Webseitenbetreiber und Internet-Service-Provider der Nutzer den Uniform Resource Locator (URL) der aufgerufen Webseiten speichern und Suchmaschinenbetreiber die eingegebene Begriffe und durch die Nutzer besuchte Treffer erfassen. Tauschen sich Nutzer via E-Mail untereinander aus, können E-Mail-Provider die Metadaten der E-Mails wie Empfänger oder Betreffzeile speichern. Solche Metadaten können mittelbar Auskunft über den Kommunikationsinhalt geben, wie die Eletronic Frontier Foundation warnend am Beispiel von Telefon-Metadaten darlegt: „They know you rang a phone sex service at 2:24 am and spoke for 18 minutes. But they don't know what you talked about. They know you called the suicide prevention hotline from the Golden Gate Bridge. But the topic of the call remains a secret. They know you spoke with an HIV testing service, then your doctor, then your health insurance company in the same hour. But they don't know what was discussed. They know you called a gynecologist, spoke for a half hour, and then called the local Planned Parenthood's number later that day. But nobody knows what you spoke about."[23]

Durch die Dokumentation der Quellensuche kommt es so zur Entstehung intellektueller Aufzeichnungen.[24] Damit wird ein Protokoll über die Gedankengänge der Menschen generiert, die sich beobachtbar manifestieren.[25]

---

19 *Bundesverband Informationswirtschaft, Telekommunikation und neue Medien e.V.*, Vor zehn Jahren wurde Facebook gegründet, 31.1.2014.

20 *The Pew Research Center for the People & the Press*, Americans Spending More Time Following the News, 12.9.2010, 105.

21 *The Pew Research Center for the People & the Press*, Americans Spending More Time Following the News, 12.9.2010, 119.

22 *The Pew Research Center for the People & the Press*, Americans Spending More Time Following the News, 12.9.2010, 93.

23 *Opsahl*, Why Metadata matters, 7.6.2013; vgl. auch eine aktuelle Studie zur Aussagekraft von Metadaten: *Parker*, Stanford students show that phone record surveillance can yield vast amounts of information, 12.3.2014.

24 *Richards*, Intellectual Privacy, 87 Texas L. Rev. (2008), 387, 436; zur Datenerhebung anlässlich von Suchmaschinennutzung und damit zusammenhängenden rechtlichen Problemen: *Ott*, Schutz der Nutzerdaten bei Suchmaschinen Oder: Ich weiß, wonach du letzten Sommer gesucht hast …, MMR 2009, 448 ff.

25 *Richards*, Intellectual Privacy, 87 Texas L. Rev. (2008), 387, 436.

Diese Aufzeichnungen erfolgen, um auf Grundlage ihrer Auswertung auf das Handeln der Nutzer zu reagieren und sie zu unterstützen oder auch zu beeinflussen. Die Daten werden genutzt, um Rückschlüsse auf die Persönlichkeit und die Interessen der Nutzer zu ziehen. Online-Anbieter bezwecken dadurch, die Nutzer durch Tracking und Profiling individuell mit Vorschlägen oder Werbung versorgen zu können.[26] Ein Resultat dieses Bemühens ist die Anpassung der im Internetkontext priorisiert angezeigten Quellen an das bisherige Rechercheverhalten der jeweiligen Nutzer. So berücksichtigen Suchmaschinenalgorithmen bei der Reihenfolge der angezeigten Ergebnisse neben anderen Einflussfaktoren auch, welche Treffer von den jeweiligen Nutzern voraussichtlich als relevantes Resultat empfunden werden dürften. Zwar führt ein bevorzugtes Ranking bestimmter Treffer meist nicht zur vollständigen Entfernung anderer. Stutzig macht allerdings, dass auch die Anzahl der gelieferten Suchergebnisse je nach Profil der Nutzer variieren kann: So erhielten in einem Beispiel von zwei Nutzern, die den identischen Begriff bei der Suchmaschine Google suchten, einer 180 Millionen Treffer, der andere 139 Millionen.[27] Jedenfalls erfordert das Auffinden von der Vorhersage abweichender Ergebnisse einen besonderen Aufwand der Nutzer, beispielsweise durch Scrollen innerhalb der Trefferliste. Niedrig gerankte Treffer können dabei als für die Nutzer faktisch nicht existent bezeichnet werden.[28]

Weiter können den Nutzern nicht nur Quellen präsentiert werden, die sie ohnehin betrachten möchten. Vielmehr vermittelt die beschriebene Datenanalyse Aufschluss darüber, welche Quellen sie wahrscheinlich betrachten wollten, wenn sie wüssten, dass sie nach ihnen suchen müssten. Es entstehen präemptive Vorhersagen.[29]

Schnittstelle zwischen den Nutzern und der Information sind dabei überwiegend Suchmaschinen.[30] Die Auswahl der vermutlich interessierenden Informationen erfolgt nicht wie bei hergebrachten Print- oder Rundfunkmedien über eine jedenfalls der eigenen Verlags- oder Senderethik verpflichtete Nachrichtenredaktion. Vielmehr kommt den Algorithmen eine Funktion zu, die der des sogenannten Agenda Setters gleicht.[31] Die Situation des Agenda Settings ist gegeben, wenn Massenmedien eine Themenhierarchie erzeugen, die einen signifikanten Einfluss auf die Themenbewertung des Publikums hat.[32] So, wie durch Agenda Setting die Vorstellung der Individuen über die Relevanz bestimmter Themen bestimmt wird, können Algorithmen Einfluss auf die den Nutzern priorisiert angezeigten Quellen und so auf ihre Vorstellung der Relevanz der Quellen nehmen. Dabei unterliegt die Trefferaus-

---

[26] Zu den technischen Hintergründen impliziter Preisgabe: siehe oben Kapitel 2,B.II.

[27] *Pariser*, Filter Bubble, 2012, 10.

[28] *Kühling/Gauß*, Suchmaschinen, ZUM 2007, 881, 883, 885.

[29] *Kerr/Earle*, Prediction, Preemption, Presumption, 66 Stanford L. Rev. Online (2013), 65, 67.

[30] *Danckert/Mayer*, Die vorherrschende Meinungsmacht von Google, MMR 2010, 219; *Kühling/Gauß*, Suchmaschinen, ZUM 2007, 881, 882.

[31] Auch wenn hier wohl eine Art personalisiertes Agenda Setting erfolgt, bei dem jeder Nutzer seine eigene Agenda erhält.

[32] *Strohmeier*, Politik und Massenmedien, 2004, 198.

wahl seit jeher der Filterung durch Suchmaschinenbetreiber, die beispielsweise Schadprogramme oder pornografische Inhalte ausblenden und eigene kommerzielle Interessen verfolgen können.[33] Weiter besteht das Geschäftsmodell von Suchmaschinen gerade darin, Zusammenhänge zwischen den Quellen zu erkennen und so die Suche zu optimieren. Es wird daher argumentiert: „It is thus hard to see how to make sense of criticisms that search engine results are 'biased' when bias is the very essence of the enterprise."[34] Dem ist jedoch entgegenzuhalten, dass auch der Kern eines Geschäfts der Kritik zugänglich sein muss, wenn er mit höherrangigen Prinzipien im Widerspruch steht.

Über die konventionelle Suchmaschinentätigkeit hinaus werden Ergebnisse verstärkt als personalisierte Suchergebnisse geliefert, auch wenn diese Form der Analyse nach einer Studie des GfK-Vereins, der 2013 rund 2.000 Deutsche befragte, bei 61 Prozent der Befragten auf Ablehnung stieß.[35] So verweist die Eingabe des Begriffs „BP" bei Google einige Nutzer priorisiert auf Investitionsmöglichkeiten bei dem Energiekonzern British Petroleum, während anderen Nutzern bevorzugt Hinweise auf das durch British Petroleum verursachte Öl-Unglück angezeigt werden.[36] Ebenso entscheiden die Algorithmen der Betreiber sozialer Netzwerke, wie beispielsweise Facebooks EdgeRank-Algorithmus, welchen Nutzern wie häufig und an welcher Stelle Informationen und Äußerungen anderer Nutzer angezeigt oder nicht angezeigt werden.[37] Der politisch links orientierte *Pariser* nennt als Beispiel, dass ihm bei Facebook keine Einträge konservativer Freunde aufgelistet werden.[38] Allein durch diese Vorgehensweise können soziale oder sonstige Missstände, auf die andere Nutzer hinweisen, als besonders gravierend erscheinen oder übersehen werden. Kommt es zu einseitigen Verweisen auf ähnliche Ansichten vertretende Quellen, wird befürchtet, dass die Nutzer von der realen Faktenlage abgeschottet werden sowie ihnen der Anreiz zu weiterem Nachdenken genommen wird, sodass sie in eine sogenannte Filter Bubble gelangen. Die Filter Bubble wird definiert als von Maschinen geschaffenes eigenes Informationsuniversum für jeden von uns.[39] Hier-

---

[33] Häufigkeit und Einflussfaktoren belegen: *Feuz/Fuller/Stalder*, Personal Web Searching in the Age of Semantic Capitalism, 16 First Monday (2011); ausführlich zum Konzept: *Bracha/Pasquale*, Federal Search Commission?, 93 Cornell L. Rev. (2008), 1149 ff.; *Chandler*, A Right to Reach an Audience, 35 Hofstra L. Rev. (2007), 1095 ff. und *Elkin-Koren*, Let the Crawlers Crawl, 76 Dayton L. Rev. (2001), 179 ff. *Yoo* leitet für die USA einen Schutz redaktioneller Anpassungen durch Onlinediensteanbieter und Suchmaschinenbetreiber durch den Ersten Zusatzartikel zur Verfassung ab aus dem Schutz redaktioneller Tätigkeit bei Zeitungen, Rundfunk, Kabelfernsehen und Telefon: *Yoo*, Free Speech and the Myth of the Internet as an Unintermediated Experience, 78 George Washington L. Rev. (2010), 697, 718 ff.

[34] *Yoo*, Free Speech and the Myth of the Internet as an Unintermediated Experience, 78 George Washington L. Rev. (2010), 697, 708.

[35] *GfK Verein*, Deutsche fürchten Datenmissbrauch, 12.11.2013, 2.

[36] *Pariser*, The Filter Bubble, 10.10.2010 und *ders.*, Filter Bubble, 2012, 10.

[37] *Cohen*, What Privacy is For, 126 Harvard L. Rev. (2013), 1904, 1913.

[38] *Pariser*, Filter Bubble, 2012, 13.

[39] *Pariser*, Filter Bubble, 2012, 17; vgl.: *Cohen*, What Privacy is For, 126 Harvard L. Rev. (2013), 1904, 1917; *Hamann/Rohwetter*, Vier Sheriffs zensieren die Welt, 2.8.2012; *Jürgens/Stark/*

bei entsteht die Gefahr der Manipulation: „The observing will affect the observed. The system watches what you do; it fits you into a pattern; the pattern is fed back to you in form of options set by the pattern; the options reinforce the pattern; the cycle begins again.“[40]

Diese Abschottung verstärkt auch den sogenannten Echokammer-Effekt: Aussagen einiger Nutzer werden von Vertretern ähnlicher Meinungen aufgegriffen, sodass sie in ihrer Überzeugung bestärkt werden und den ähnlich Denkenden wiederum das Gefühl geben, ihre Meinung entspräche der Realität. Anstatt auf gegenläufige Meinungen zu stoßen, geraten die Nutzer in sogenannte Feedback-Schleifen,[41] die eben jene Echokammern der Gedanken[42] erzeugen. Bestehende Ansichten der Nutzer werden bestärkt und der Horizont verengt. Es entsteht ein „groupthink ghetto“.[43] Der Effekt wird weiter unterstützt durch das Phänomen der sogenannten Bestätigungsfehler, also durch die Neigung, Informationen für richtig zu halten, die die eigene Sicht stärken und überdies schwerpunktmäßig nur das zu sehen, was man sehen möchte.[44] Eine Rolle spielt zudem der aus der Verhaltenspsychologie bekannte Effekt, Aussagen als wahr anzusehen, wenn man vorher schon einmal davon gehört hat. So belegt eine Studie aus dem Jahr 1977, welche die Teilnehmer im Zwei-Wochen-Abstand Fragen beantworten ließ, dass Behauptungen unabhängig von ihrer Richtigkeit mit erhöhter Wahrscheinlichkeit als zutreffend angesehen werden, wenn die Frage häufiger gestellt wird.[45] Es ist davon auszugehen, dass dieser Effekt durch die überproportionale Konfrontation mit Bekanntem durch personalisierte Quellenangebote verstärkt wird. Personalisierte Suchergebnisse berücksichtigen dabei nicht nur die eigene Suchhistorie der Nutzer, sondern greifen auch auf statistische Gruppenprofile zurück, sodass die Nutzer sogar in für sie vollständig neuen Bereichen bevorzugt Quellen angezeigt bekommen, die auf ihr Alter, die Herkunft, den Vermögensstand et cetera ausgerichtet sind.[46]

Quellenselektion kann dem Komfort der Nutzer dienen oder der Durchsetzung wirtschaftlicher oder politischer Interessen, die bestimmte Meinungen verstärken oder unterdrücken möchten. Anders als beispielsweise die politische Färbung einer bewusst aus diesem Grund gelesenen Zeitung ist die Vorselektion im Internet den

---

Magin, Gefangen in der Filter Bubble?, in: Stark/Dörr/Aufenanger (Hrsg.), Die Googleisierung der Informationssuche, 2014, 98 ff.; *Lewandowski/Kerkmann/Sünkler*, Wie Nutzer im Suchprozess gelenkt werden, in: Stark/Dörr/Aufenanger (Hrsg.), Die Googleisierung der Informationssuche, 2014, 75 ff. und *Schmitt*, Automatisch vorsortiert, 22.6.2011.

40 *Lessig*, Code, 2006, 220.

41 *Dwork/Mulligan*, It's Not Privacy, And It's Not Fair, 66 Stanford L. Rev. Online (2013), 35, 37.

42 *Richards/King*, Three Paradoxes of Big Data, 66 Stanford L. Rev. Online (2013), 41, 44.

43 *Saletan*, Bubble Think, 3.5.2010.

44 *Pariser*, Filter Bubble, 2012, 93, 96.

45 *Hasher/Goldstein/Toppino*, Frequency and the Conference of Referencial Validity, 16 J. of Verbal Learning and Verbal Behaviour (1977), 107 ff.

46 *Feuz/Fuller/Stalder*, Personal Web Searching in the Age of Semantic Capitalism, 16 First Monday (2011).

Nutzern regelmäßig nicht bewusst.[47] Daher ist es unzutreffend, die Gefahren der Filter Bubble mit denen der Filterung durch Offline-Redaktionen gleichzustellen.[48] *Pariser* führt vielmehr richtig aus: „Google sagt Ihnen aber nicht, für welche Person er Sie hält und warum er Ihnen die Ergebnisse zeigt, die Sie auf Ihrem Bildschirm sehen. Sie wissen nicht, ob die Annahmen zu Ihrer Person stimmen – Sie wissen vielleicht nicht einmal, dass Annahmen zu Ihrer Person getroffen werden."[49] Dieser Mangel an Transparenz sowie die mangelnde Wahlmöglichkeit (anders als bei der Entscheidung zur Lektüre einer bestimmten Zeitung entscheiden sich Nutzer nicht für die personalisierte Suche unter Verwendung einer intransparenten Kategorie, in die sie eingeordnet werden) führen dazu, dass die Nutzer kaum effektive Maßnahmen ergreifen können, um der Beeinflussung zu entgehen. Gleichzeitig wird ihr Hang zu weiteren Erkundungen gebremst, da ihnen scheinbar bereits ausreichend relevante Informationen geliefert werden. „Wenn der eigene Teller schon voller schmackhafter Informationen ist, muss man nicht mehr über seinen Rand hinausschauen."[50] So ist eine unmerkliche Lenkung der Individuen in eine Richtung und damit eine Behinderung des Erkundungsprozesses denkbar.

Die Nutzung der Aufzeichnung und die Auswertung des Internet-Erkundungsprozesses können demnach dazu führen, dass den Nutzern keine neutrale Auswahl an Quellen zur Verfügung steht. Die Quellen werden vielmehr an die wirklichen oder angenommenen Interessen der Nutzer angepasst, die ihre Interessen wiederum in der Konsequenz an die durch die Quellen vorgegebene Richtung angleichen, was durch die sodann angebotenen Quellen bestärkt wird. „Wenn eine sich selbst erfüllende Prophezeiung eine falsche Annahme über die Welt ist, die sich durch die eigenen Handlungen bewahrheitet, so stehen wir nun vor sich selbst erfüllenden Identitäten: Das verzerrte Persönlichkeitsprofil des Internets wird zu unserem wahren Ich."[51]

Die dargestellten, in der Literatur befürchteten Konsequenzen informationeller Preisgabe erscheinen plausibel und ihr Eintritt wahrscheinlich. Demnach besteht das realistische Risiko, dass die Internetrecherche nur eine beschränkte Auswahl an Fakten umfasst, wodurch auch der folgende intellektuelle Erkenntnisprozess von vornherein limitiert ist.

2. Selbstzensur

Elektronische Aufzeichnungen über intellektuelle Aktivitäten könnten in ihren Wirkungen konventioneller physischer Überwachung vergleichbar sein und zu

---

[47] *Horn*, Das Netz als ethische Herausforderung, 542 Politische Studien (2013), 54, 60 f.
[48] So aber: *Kappes*, Warum die Gefahren der Filter Bubble überschätzt werden, 5.2012, 3.
[49] *Pariser*, Filter Bubble, 2012, 18.
[50] *Pariser*, Filter Bubble, 2012, 102.
[51] *Pariser*, Filter Bubble, 2012, 120.

Selbstzensur führen (siehe a)), welche sich auf die Quellenauswahl (siehe b)) und den Erkenntnisprozess auswirken könnte (siehe c)).

Die Verwendung personenbezogener Daten durch Dritte kann für die Nutzer – wie einleitend zu diesem Kapitel festgestellt – zu vielfältigen tatsächlichen Nachteilen führen. Der Fokus soll im Folgende darauf liegen, inwiefern die Angst vor der Entstehung solcher tatsächlicher Nachteile die Persönlichkeitsentwicklung beeinträchtigen kann.

a) Zusammenhang zwischen Überwachung und Selbstzensur

In einem ersten Schritt soll das Wechselspiel zwischen automatisierter Datenverarbeitung und dem Einschüchterungseffekt, der zu Selbstzensur führen könnte, beleuchtet werden.

Obwohl dieses Argument vielfach, unter anderem auch durch das Bundesverfassungsgericht,[52] verwendet wird, ist die empirische Basis bemerkenswert dünn. Die Korrelation ist empirisch schwer greifbar,[53] die in Rede stehenden Auswirkungen jedoch immens. Um einen wirksamen Grundrechtsschutz zu gewährleisten, muss daher unter Ausschöpfung der Einschätzungsprärogative des Staates auch nachvollziehbar darlegbaren, wahrscheinlichen Konsequenzen Beachtung geschenkt werden. So ist das Argumentieren mit plausiblen Besorgnissen im Recht nichts Ungewöhnliches, wie sich beispielsweise daran zeigt, dass das Wahlgeheimnis „Ausdruck von Sorgen gegenüber einem Staat [ist], der als Rechtsstaat eigentlich keinen Anlass zu ihnen geben sollte."[54]

Unter dem Begriff der Überwachung versteht man ein „set of practices that gather and collect data about individuals or entities, with or without their knowledge or consent, for purposes of an analysis which sorts those individuals or entities on basis of their behavior or characteristics."[55] Sowohl physische Überwachung (beispielsweise durch Verfolgung) als auch Internetüberwachung lassen sich unter diese Definition fassen. Informationelle Preisgabe löst im Regelfall keine physische Überwachung aus, unter Umständen aber die Aufzeichnung und Auswertung aller Tätigkeiten im Internetkontext, mit und ohne Wissen der Privatheitsträger im konkreten Fall.

Dass die Preisgabe personenbezogener Daten dazu führt, dass diese Anderen bekannt werden, ist kein spezifisches Risiko der Internetnutzung. Doch bieten im reinen Offline-Kontext das begrenzte Erinnerungsvermögen der Empfänger sowie häufig die praktische Unauffindbarkeit von in der Vergangenheit preisgegebenen

---

[52] Hervorzuheben sind hier insbesondere die Ausführungen im Volkszählungsurteil, BVerfGE 65, 1 (43).

[53] Zu dieser Kritik mit weiteren Nachweisen: *Schwabenbauer*, Heimliche Grundrechtseingriffe, 2013, 142 f.

[54] *Schwabenbauer*, Heimliche Grundrechtseingriffe, 2013, 144 ff.

[55] *Johnson/Wayland*, Surveillance and transparency as sociotechnical systems of accountability, in: Haggerty/Samatas (Hrsg.), Surveillance and Democracy, 2010, 19, 23.

personenbezogenen Daten einen Schutz informationeller Privatheit. Zum Schutz vor Überwachung führt eine der Concurring Opinions in United States v. Jones aus: „In the pre-computer age, the greatest protections of privacy were neither constitutional nor statutory, but practical. Traditional surveillance for any extended period of time was difficult and costly and therefore rarely undertaken."[56] Es kann der Vergleich gezogen werden von konventioneller (Offline-)Datenverarbeitung zu einer Flaschenpost im offenen Meer. Diese ist zwar vorhanden und allgemein für jedermann zugänglich, bewirkt jedoch keine Kommunikation.[57] Eine Konsequenz technisch unbegrenzter Speicher- und Auswertungsmöglichkeiten ist hingegen die leichte Auffindbarkeit bisher praktisch verborgener Daten. Es wird daher – ohne dass sich diese Terminologie bisher durchgesetzt hätte – treffend dafür plädiert, bei dem Zugänglichwerden solcher Daten vom Verlust der Obskurität anstelle des Verlusts der Privatheit zu sprechen.[58]

Angesichts der Allgegenwärtigkeit automatisierter Datenverarbeitung entstehen umfassende Datenmengen über die Individuen. Deren Erhebung, Verarbeitung und Nutzung erfolgen sowohl durch private als auch durch staatliche Akteure, wobei zusehends staatliche Stellen auch Zugriff auf private Datensammlungen erhalten.[59] Dies kann einem breiten Publikum zugängliche Sammlungen betreffen, beispielsweise öffentliche Profile in sozialen Netzwerken. Ebenso können sich Ermittlungsbehörden wie auch Geheimdienste in rechtlich sanktionierten Fällen Zugang zu privaten Datensammlungen verschaffen[60] – im Rahmen von Amtshilfe oder geheimdienstlichen Aktivitäten auch über Ländergrenzen hinweg.

So entwickelt sich die Gesellschaft hin zu einer, in der durch eine Vielzahl von Akteuren umfassende Aufzeichnungen und Auswertungen der Internetaktivitäten der Nutzer getätigt werden. Diesen Zusammenhang macht der Begriff „dataveil-

---

[56] United States v. Jones, 132 S.Ct. 945, 963 (2012) (*Alito*, *Ginsburg*, *Breyer*, *Kagan*, *JJ*., concurring).

[57] *Kamlah*, Hinweise aus der Rechtsprechung des Bundesverfassungsgerichts zur Regelung eines materiellen Informationsrechts, in: Steinmüller (Hrsg.), Informationsrecht und Informationspolitik, 1976, 196, 197.

[58] *Hartzog/Selinger*, Obscurity, 17.1.2013.

[59] *Richards*, The Dangers of Surveillance, 126 Harvard L. Rev. (2013), 1934, 1940 f. Ein besonders umfassendes Beispiel ist die Vorratsdatenspeicherung von Telekommunikationsverkehrsdaten, siehe dazu jüngst: EuGH EuZW 2014, 459 ff.; einen Überblick über das Gesetzgebungsverfahren zur erneuten Einführung der Vorratsdatenspeicherung in Deutschland bietet: *Redaktion MMR-Aktuell*, Vorratsdatenspeicherung im Gesetzgebungsverfahren, MMR-Aktuell 2015, 369589 ff.

[60] *Masing*, Herausforderungen des Datenschutzes, NJW 2012, 2305, 2309. Durch Überwachung kann ein Ungleichgewicht im Kräfteparallelogramm zwischen Überwachern und Überwachten entstehen, das die Überwacher missbrauchen können, *Richards*, The Dangers of Surveillance, 126 Harvard L. Rev. (2013), 1934, 1935, 1953 ff. Ein Nichtbeachtung der Grenze zwischen für die Behörden frei verfügbaren Daten und solchen, auf die nur aufgrund gesetzlicher Anordnung zugegriffen werden darf, ist jedoch nicht originär eine Gefahr informationeller Preisgabe, sondern der Einhaltung der Gesetzesbindung staatlichen Handelns.

lance“[61] plakativ deutlich – eine Zusammensetzung aus „data“ und „surveillance“. Automatisierte Datenverarbeitung kann so ein Gefühl des Überwachtwerdens entstehen lassen, das mit dem durch physische Überwachung ausgelösten vergleichbar ist.[62]

Diese theoretisch allgegenwärtige Möglichkeit der Überwachung konfligiert mit dem menschlichen Bestreben, bei Anderen ein wohlwollendes Bild der eigenen Person zu erzeugen. Die Einzelnen wollen (wenn auch nicht immer bewusst) im Regelfall sympathisch, intelligent, weise und vorausschauend wirken. Fehler, Meinungsumschwünge und Angreifbares sollen verborgen bleiben.

Die Effekte dieses Bestrebens lassen sich auch systemtheoretisch näher bestimmen:[63] Ausgehend von der Annahme verschiedener gesellschaftlicher Teilsysteme konstituiert sich nach *Luhmann* die menschliche Identität dynamisch im sozialen, das heißt kommunikativen Austausch mit anderen Individuen, bei welchem zur Vereinfachung Rollenbilder und -erwartungen genutzt werden. Individualität ist dabei eine von den Individuen erwartete Leistung.[64] Erst die Wahrnehmung eines Verhaltens als einer bestimmten Rolle zugehörig macht diese Rolle als Teilaspekt der Person aus und schreibt sie damit in gewisser Weise fest. Die situationsgebundene Rollenidentität entspricht dabei nicht der persönlichen Identität, trägt jedoch zu ihrer Konstituierung bei. Durch Selbstdarstellung können die Einzelnen in Kommunikation mit anderen zur Person werden. Kommunikation ist daher so etwas wie die regelmäßige Bestätigung und Aktualisierung bestehender Rollenbilder und -erwartungen. „Der Mensch wird die Persönlichkeit, als welche er sich darstellt.“[65] Gleichzeitig kann aber jedes Missgeschick Auswirkungen über die Situation hinaus haben, weil Rückschlüsse auf die persönliche Identität gezogen werden. *Luhmann* bemerkt dazu: „Daß jener Schluss auch gezogen wird, wenn er falsch ist, beweist im übrigen, daß er, wenn er zutrifft, nicht deswegen gezogen wird, weil er zutrifft. Ob falsch oder richtig, der Schluß verrät das soziale Interesse an der Protektion fremder Selbstdarstellungen.“[66] Jedes situationsgebundene Handeln erfolgt somit vor dem Hintergrund, dass die persönliche Identität durch inkonsistente oder peinliche Rückschlüsse bedroht werden kann. *Luhmann* folgert: „Mit jeder Kommunikation riskiert der Mensch seine Würde. In Anwesenheit Anderer muß er sich zusammen-

[61] Zuerst verwendet von: *Clarke*, Information Technology and Dataveillance, 11.1987.

[62] So auch: *Nehf*, Recognizing the Societal Value in Information Privacy, 78 Washington L. Rev. (2003), 1, 9 und *Solove*, “I’ve Got Nothing to Hide” and Other Misunderstandings of Privacy, 44 San Diego L. Rev. (2007), 745, 765. Entsprechend werden beide häufig ohne weitere Begründung gleichgesetzt, z. B.: *Hansen*, Überwachungstechnologie, in: Schmidt/Weichert (Hrsg.), Datenschutz, 2012, 78 und *Nissenbaum*, Privacy as Contextual Integrity, 79 Washington L. Rev. (2004), 119, 120.

[63] Zu den folgenden Ausführungen, soweit nicht anderweitig angegeben: *Luhmann*, Grundrechte als Institution, 1965, 60 ff.

[64] *Trute*, Verfassungsrechtliche Grundlagen, in: Roßnagel (Hrsg.), Handbuch Datenschutzrecht, 2003, 156, 167.

[65] *Luhmann*, Grundrechte als Institution, 1965, 60.

[66] *Luhmann*, Grundrechte als Institution, 1965, 62.

nehmen. Er kann nicht jede Körperbewegung vollziehen, nicht jedem Bedürfnis nachgehen. Er hat seine Worte abzuwägen und nicht zu viel von sich preiszugeben. Und er muß gegen Einsicht schützen, was verborgen bleiben soll."[67] *Luhmann* liefert damit eine überzeugende Bestimmung des menschlichen Interesses daran, das eigene Verhalten an die Perspektive der Umwelt anzupassen.

Die Auswirkung von Überwachung auf menschliches Verhalten kann wie folgt deutlich gemacht werden: „Imagine now being watched by an officer […] every time you walk through certain streets. Say you want to run (to catch a bus, for a brief bit of exercise or just for the hell of it). Will you? Or assume you want to obscure your face (because of the wind or a desire to avoid being seen by an officious acquaintance)? How about hanging out on the street corner (waiting for friends or because you have nothing else to do)? In all of these scenarios, you will probably feel and perhaps act differently than when the officer is not there. Perhaps your hesitancy comes from uncertainty as to the officer's likely reaction or simply from a desire to appear completely law-abiding; the important point is that it exists."[68]

Auch *Orwell* nimmt sich des Zusammenhangs zwischen theoretischer Möglichkeit allgegenwärtiger Überwachung und Anpassung menschlichen Verhaltens daran an, wenn er in „Nineteen Eighty-Four" ausführt: „There was of course no way of knowing whether you were being watched at any given moment. […] It was even conceivable that they watched everybody all the time. […] You had to live – did live, from habit that became instinct – in the assumption that every sound you made was overheard, and, except in darkness, every movement scrutinized".[69] Die Angst vor Überwachung führt so zu einer Verhaltensanpassung.

Auf die Nutzer übertragen, lässt sich annehmen, dass diese, wenn sie ständige Überwachung befürchten müssen, negative Folgen für die persönliche Identität verhindern möchten. Häufig werden sie versuchen, ihren Überwachern gegenüber in positivem Licht zu erscheinen.[70] Dieses Bestreben wird, wenn auch etwas undifferenziert, aufgegriffen, indem der „kategorische Imperativ des digitalen Zeitalters" aufgestellt wird: „Handele stets so, dass Dir die öffentlichen Effekte Deines Handelns langfristig vertretbar erscheinen."[71]

Die Nutzer befinden sich in einem Interessenkonflikt. Einerseits sind sie bestrebt zu verhindern, dass Andere negative Schlüsse über sie ziehen, die ihnen zum Nachteil gereichen könnten. Andererseits können sie nicht abschätzen, welche Daten über sie im Laufe der Jahre in wessen Hände geraten und was aus diesen durch automatisierte Datenverarbeitung gefolgert wird. *Solove* erklärt das Gefühl der Ohnmacht hinsichtlich der Unkontrollierbarkeit automatisierter Datenverarbeitung anhand der Situation, in der sich die Hauptfigur *Josef K.* in *Kafkas* „Der Prozess" be-

---

[67] *Luhmann*, Grundrechte als Institution, 1965, 67.
[68] *Slobogin*, Public Privacy, 72 Mississippi. L.J. (2002), 213, 241 f.
[69] *Orwell*, Nineteen Eighty-Four, 1990 (Original: 1949), 2.
[70] *Slobogin*, Public Privacy, 72 Mississippi. L.J. (2002), 213, 238 ff. m.w.N.
[71] *Porksen/Detel*, Der entfesselte Skandal, 2012, 233.

findet: „the problem is […] a suffocating powerlessness and vulnerability created by the court system [… and] its exclusion of the protagonist from having any knowledge or participation in the process."[72] Der Beschränkung des US-Grundrechtsschutzes gegen staatliches Handeln[73] Rechnung tragend, bezieht sich *Solove* auf Datensammlungen durch Behörden. Gleichwohl lässt sich der Vergleich übertragen auf das Handeln Privater. Nach erstmaliger Preisgabe ihrer Daten sehen sich die Nutzer einem diffusen System an Datenverarbeitern gegenüber: Es kommt zu einem Kontrollverlust. Die Konsequenzen können für sie ebenso unüberschaubar sein wie für *Josef K.* der Ausgang des Prozesses.[74]

Jedenfalls zeigen diese Beispiele in überzeugender Weise, wie das Gefühl ständiger Überwachung zu einer Verhaltensanpassung führen kann.

Da Nutzer nicht vorhersehen können, was in Zukunft als verfehlt angesehen werden wird, können sie dem Dilemma selbst durch heute makelloses Verhalten nicht entrinnen. Doch es besteht die Möglichkeit zur bewussten oder unbewussten Abmilderung. Das Risiko unangenehmen Auffallens sinkt erheblich durch konformistische Anpassung der Handlungsweisen an die vermeintliche Norm. So entsteht ein Prozess der Selbst-Überwachung, in dem die Einzelnen in vorauseilendem Gehorsam Selbstzensur üben, um hypothetischen, ihnen noch unbekannten Gefahren zu entgehen.[75]

Veranschaulichen lässt sich das Szenario der vorauseilenden Selbstüberwachung am Beispiel des von *Bentham* entwickelten und von *Foucault*[76] auf die Gesellschaft der 1970er Jahre übertragenen Panopticons. Dieses stellt ein Gebäude dar, in dem den Beobachteten keine Privatsphäre zugestanden wird. Die räumliche Anordnung – ein runder, von jederzeit lichtdurchfluteten Zellen umschlossener Hof, in dessen Mitte ein von den Zellen aus nicht einsehbarer Überwachungsturm steht – bedingt es, dass kein Ort existiert, an dem die Zelleninsassen vor dem Blick der Wächter sicher wären.[77] Die Insassen können nie wissen, ob sie beobachtet werden. So entsteht ein Gefühl permanenter Überwachtheit. Nicht die tatsächliche Beobachtung, sondern die Angst vor ihr löst Verunsicherung und Gehorsam aus.[78] *Foucault* beschreibt diese Wirkung als „Schaffung eines bewußten und permanenten Sichtbar-

---

[72] *Solove*, "I've Got Nothing to Hide" and Other Misunderstandings of Privacy, 44 San Diego L. Rev. (2007), 745, 766; ausführliche Herleitung: *ders.*, Privacy and Power, 53 Stanford L. Rev. Online (2001), 1393, 1419 ff. und *ders.*, Nothing to Hide, 2011, 26 f.

[73] Siehe unten Kapitel 5,B.

[74] *Nehf* hingegen zweifelt zurecht diese Methaper an, da Nutzer, anders als *Josef K.*, die Situation selbst wählten. Richtig sei stattdessen ein Vergleich mit *Hänsel* und *Gretel*, die dazu verführt werden, sich in Gefahr zu begeben: *Nehf*, Recognizing the Societal Value in Information Privacy, 78 Washington L. Rev. (2003), 1, 11.

[75] So auch: *Kang*, Information Privacy in Cyberspace Transactions, 50 Stanford L. Rev. Online (1998), 1193, 1216 f. und *Solove*, Understanding Privacy, 2009, 108 f.

[76] Zu den folgenden Ausführungen, soweit nicht anders angegeben: *Foucault*, Überwachen und Strafen, 1976, 256 ff.

[77] *Bentham*, Panoptikum oder Das Kontrollhaus, 2013 (Original: 1791), 13 ff.

[78] *Bentham*, Panoptikum oder Das Kontrollhaus, 2013 (Original: 1791), 12.

keitszustandes beim Gefangenen, der das automatische Funktionieren der Macht sicherstellt. Die Wirkung der Überwachung ist permanent, auch wenn ihre Durchführung sporadisch ist; die Perfektion der Macht vermag ihre tatsächliche Ausübung überflüssig zu machen; […] die Häftlinge sind Gefangene einer Machtsituation, die sie selber stützen."[79]

Die Insassen internalisieren das Machtverhältnis und werden zum Prinzip ihrer eigenen Unterwerfung. Zur Vermeidung einer möglichen Bestrafung verändern sie ihr Verhalten und werden ihr eigener Wächter. Unerheblich sind dabei Person und Motiv der Aufseher. Umso mehr mögliche wechselnde anonyme Beobachter es gibt, umso größer ist die Unsicherheit für die Insassen.

Das Panopticon ist dabei nach *Foucault* ein verallgemeinerungsfähiges Funktionsmodell der perfektionierten, automatisierten und entindividualisierten Machtausübung. Er schließt mit den Worten: „Was ist daran verwunderlich, wenn das Gefängnis den Fabriken, den Schulen, den Kasernen, den Spitälern gleicht, die allesamt den Gefängnissen gleichen?"[80] Auf die Gesellschaft der 1970er Jahre als „Disziplinargesellschaft"[81] und „Gesellschaft der Überwachung"[82] übertragen, zeige das Panopticon, wie diese Gesellschaft die Individuen „sorgfältig fabriziert […,] eingeschlossen in das Räderwerk der panoptischen Maschine, das wir selbst in Gang halten – jeder ein Rädchen."[83]

Vergleichbar dem Verhalten im Panopticon können Nutzer, wenn sie nicht über die Preisgabe und Verwendung ihrer personenbezogenen Daten bestimmen können und damit nicht wissen, welche Schlüsse aus den Daten gezogen und welche Handlungen in Zukunft als unangemessen betrachtet werden, aus Angst und vorauseilendem Gehorsam Selbstzensur üben.[84] Die vorgetragenen Bedenken überzeugen und es erscheint wahrscheinlich, dass schon die bloße Angst vor einer Aufzeichnung der Onlineaktivitäten der Nutzer zu Selbstzensur führt.

b) Selbstzensur hinsichtlich der Quellenauswahl

Die beschriebene Selbstzensur könnte sich zunächst auf die Auswahl der berücksichtigten Quellen auswirken.

---

[79] *Foucault*, Überwachen und Strafen, 1976, 258.
[80] *Foucault*, Überwachen und Strafen, 1976, 292.
[81] *Foucault*, Überwachen und Strafen, 1976, 279.
[82] *Foucault*, Überwachen und Strafen, 1976, 278.
[83] *Foucault*, Überwachen und Strafen, 1976, 279.
[84] So auch: *Heller*, Post-Privacy, 2011, 100 und *Kahmann*, Überwachen und Strafen im Internet, in: Venhaus/Haselbeck/Wintermann (Hrsg.), Globalisierung im Schatten der Überwachung, 2013, 65, 66; vgl. bereits die dem Volkszählungsurteil zugrunde liegenden Überlegungen: „Wer nicht mit hinreichender Sicherheit überschauen kann, welche ihn betreffende Informationen in bestimmten Bereichen seiner sozialen Umwelt bekannt sind, und wer das Wissen möglicher Kommunikationspartner nicht einigermaßen abzuschätzen vermag, kann in seiner Freiheit wesentlich gehemmt werden, aus eigener Selbstbestimmung zu planen oder zu entscheiden.", BVerfGE 65, 1 (43).

Angesichts der Speicherung und Auswertung versandter Rechercheanfragen, beispielsweise im Rahmen von Suchmaschinennutzung, müssen Nutzer damit rechnen, dass jede Suchanfrage Grundlage für Persönlichkeitsprofile wird, mit denen sie konfrontiert werden können oder die ohne ihr Wissen, auch zu ihren Ungunsten, verwendet werden können.[85] Dies illustriert eine 2013 durchgeführte Studie, die 528 US-amerikanische Journalisten zu ihrem Internetverhalten befragte. 16 Prozent gaben an, aus Angst vor Internetüberwachung davon abgesehen zu haben, Suchmaschinenanfragen zu stellen oder Webseiten zu besuchen; 12 Prozent haben dies jedenfalls erwogen.[86]

Noch deutlicher macht es eine, im Unterschied zu vielen anderen nicht auf eigenen Angaben von Teilnehmern beruhende, Studie, die das Suchverhalten der Google-Nutzer während des gesamten Jahres 2013 in elf Ländern (USA, Kanada, China, Mexiko, Japan, Deutschland, Südkorea, Großbritannien, Frankreich, Brasilien und Saudi-Arabien) auf Veränderungen untersuchte, die zeitlich mit dem öffentlich Bekanntwerden der NSA-Überwachungstätigkeiten im Juni 2013 korrelieren.[87] Untersucht wurde, ob sich Veränderungen in der Suche nach 282 ausgewählten Begriffen feststellen lassen. Dafür wurden drei Kategorien gebildet: Zunächst wurde aus einer Liste von Begriffen, die das US Department for Homeland Security als verdächtige Begriffe listet,[88] ein Pool von Termini gewonnen, die den Nutzern Probleme mit der US-Regierung einbringen könnten. Weiter wurde eine im Wege des Crowdsourcings erstellte Liste von Wörtern, die bei Bekanntwerden der Suche nach ihnen im sozialen Umfeld als peinlich empfunden werden,[89] als sozial peinlich kategorisiert. Und schließlich wurden neutrale Suchbegriffe analysiert, die aus einer von Google selbst veröffentlichten Liste der 50 meistgesuchten Wörter entstammen.[90] Innerhalb der ersten beiden Kategorien wurde dann eine zusätzlich Abstufung darüber vorgenommen, wie unangenehm den Betroffenen ein Bekanntwerden der Suche nach den Begriffen werden kann. Es zeigte sich:

– Die Suche nach neutralen Begriffen nahm seit Juni 2013 bei insgesamter Betrachtung sowie der Betrachtung der Werte nur in den USA und nur in Deutschland zu.[91]
– Seit Juni 2013 wurde bei Betrachtung in toto sowie bei Fokus nur auf die USA weniger nach Termini gesucht, die zu Problemen mit der US-Regierung führen

---

[85] *van Hoboken* leitet den Schutz vor Einschüchterungseffekten, die mangelnde informationelle Privatheit bei der Suchmaschinennutzung haben kann, aus entsprechenden rechtlich abgesicherten Erwägungen bei der Bibliotheksnutzung her: *van Hoboken*, Search engine freedom 2012, 165 f., 294.

[86] *FDR Group*, The Impact of US Government Surveillance on Writers, 31.10.2013.

[87] *Marthews/Tucker*, Government Surveillance and Internet Search Behavior, 24.03.2014.

[88] *Marthews/Tucker*, Government Surveillance and Internet Search Behavior,24.03.2014, 33 f.

[89] *Marthews/Tucker*, Government Surveillance and Internet Search Behavior, 24.03.2014, 35 f.

[90] *Marthews/Tucker*, Government Surveillance and Internet Search Behavior, 24.03.2014, 37.

[91] *Marthews/Tucker*, Government Surveillance and Internet Search Behavior, 24.03.2014, 13 f.

können. In Deutschland blieb die Zahl im Wesentlichen unverändert, hatte jedoch nicht an dem Anstieg teil, den die neutralen Schlagworte erfuhren.[92]

– Die Suche nach Begriffen, die sozial als unangenehm empfunden werden können, nahm insgesamt und bei Betrachtung der US-Werte ab. In Deutschland hingegen war ein Anstieg zu verzeichnen, der jedoch geringer ausfiel als der Anstieg der Suche nach Begriffen, die sozial nicht als unangenehm empfunden werden.[93]

Erstaunlich ist, dass das vage Wissen um Überwachungstätigkeiten durch einen US-Geheimdienst zum einen auch das Suchverhalten nicht-amerikanischer Nutzer zu hemmen scheint (auch wenn viele von diesen jedenfalls in keinem direkten Verhältnis zum US-amerikanischen Staat stehen) und dass zum anderen generell eine gewisse Selbstzensur geübt zu werden scheint auch hinsichtlich solcher Begriffe, die zwar allgemein peinlich sein können, aber keinerlei strafrechtliche Bewandtnis haben. Umso mehr ist davon auszugehen, dass ein diffuses Gefühl der Beobachtung zu weitreichender Limitierung des Suchverhaltens führen kann, die über rational zwingende Einschränkungen hinausgeht.

Ähnliches zeigt auch eine Befragung des Pew Research Centers von 475 Probanten im Januar 2015: In dieser gaben 17 Prozent derjenigen, die von den Online-Überwachungen der NSA gehört hatten, an, als Reaktion darauf ihr Suchmaschinenverhalten geändert zu haben.[94]

Diese Form der Selbstzensur trifft insbesondere Bevölkerungsgruppen, die aufgrund abstrakter Merkmale leichter in den Verdacht geraten, sich abseits der Norm zu bewegen. So wurde im Jahr 2007 untersucht, wie sich die verstärkte Internetüberwachung in den Vereinigten Staaten als Reaktion auf die Anschläge vom 11. September 2001 auf das Internetverhalten US-amerikanischer Muslime auswirkte. Bei einer Befragung von 311 US-amerikanischen Muslimen zeigte sich, dass 11,6 Prozent ihr Verhalten im Allgemeinen als Reaktion auf befürchtete staatliche Überwachung verändert hatten (leichte Veränderungen: 6,1 Prozent, mäßige Veränderungen: 2,3 Prozent, viele Veränderungen: 1,6 Prozent, signifikante Veränderungen: 1,6 Prozent).[95] 8,4 Prozent der Befragten hatten angesichts der Furcht vor Internetüberwachung ihr Internetverhalten geändert (leichte Veränderungen: 3,9 Prozent, mäßige Veränderungen: 1,6 Prozent, viele Veränderungen: 1,9 Prozent, signifikante Veränderungen: 1 Prozent), wobei von dieser Gruppe 57,6 Prozent auf den Besuch bestimmter Webseiten verzichtet hatten aus Angst vor staatlicher Überwachung.[96] Schließlich gaben 11,9 Prozent an, persönlich einen anderen US-amerikanischen Muslim zu kennen, der aus Angst vor staatlicher Internetüberwachung

---

[92] *Marthews/Tucker*, Government Surveillance and Internet Search Behavior, 24.03.2014, 13 f.

[93] *Marthews/Tucker*, Government Surveillance and Internet Search Behavior, 24.03.2014, 15 f.

[94] *Rainie/Madden*, Americans' Privacy Strategies Post-Snowden, 16.3.2015, 17.

[95] *Sidhu*, The Chilling Effect of Government Surveillance Programs on the Use of the Internet by Muslim-Americans, 7 Univ. of Maryland L. J. of Race, Religion, Gender (2007), 375, 391.

[96] *Sidhu*, The Chilling Effect of Government Surveillance Programs on the Use of the Internet by Muslim-Americans, 7 Univ. of Maryland L. J. of Race, Religion, Gender (2007), 375, 391.

sein Online-Verhalten verändert hatte.[97] Gerade diejenigen, die aufgrund eines beliebigen Merkmals aus dem gesellschaftlichen Durchschnitt herausstechen, sind also insbesondere anfällig für die beschriebene Selbstzensur.

Im Bestreben um die Vermeidung künftiger Nachteile ist daher eine Anpassung an die wahrscheinliche Perspektive der Überwacher zu erwarten. Es besteht die Gefahr, dass die Nutzer schon bei der Selektion der Quellen, die als Grundlage ihres intellektuellen Erkenntnisprozesses dienen, von der Norm abweichende Quellen außer Acht lassen. So mag es – auch ohne Nachahmungsabsicht – möglicherweise von Interesse sein zu wissen, wie Bomben hergestellt, kinderpornografische Webseiten aufgebaut oder Argumentationen in rechtsradikalen Foren strukturiert werden. Es ist jedoch denkbar, dass den Einzelnen das Bekanntwerden derartiger Suchanfragen unangenehm wäre und sie diese folglich unterlassen. So kann der Erkenntnisprozess dadurch behindert werden, dass sich die Nutzer schon bei der Auswahl ihrer Quellen selbst einschränken.

Es erscheint daher wahrscheinlich, dass das Risiko der Aufzeichnung von Internetaktivitäten im Bestreben um die Vermeidung hypothetischer Nachteile zur Selbstzensur hinsichtlich der berücksichtigten Quellen führt.

a) Selbstzensur hinsichtlich des Erkenntnisprozesses

Die Angst vor Überwachung der Internetaktivitäten könnte zudem nicht nur die Quellenauswahl beeinflussen, sondern auch zur Beschränkung der gefassten Ideen führen, wenn die Nutzer aus dieser Angst heraus Selbstzensur hinsichtlich der Entwicklung von Ideen üben.

Zur Entwicklung neuer Ideen trägt – neben einem neutralen Angebot an Quellen[98] und deren angstfreier Nutzung[99] – die Möglichkeit zu freiem, unbeobachteten Denken sowie zur Kommunikation mit Vertrauten bei.

Zunächst ist für den Ideenentwicklungsprozess die Freiheit des Denkvorgangs notwendig. Als Entwicklungsvoraussetzung autonomer Persönlichkeiten wird daher ein „Wechselspiel von Selbstdistanzierung, Selbstvergewisserung und Selbstannahme" angesehen.[100] Bedingung ist die informationelle Autonomie als der Zustand, in dem keinerlei Informationen über nicht-anonyme Entscheidungen gespeichert werden.[101] Es bedarf Freiräumen der experimentellen Selbsterprobung zum Zweck der Selbsterkundung und Selbstprüfung.[102] Individuen gehen ihrer Neugier-

---

[97] *Sidhu*, The Chilling Effect of Government Surveillance Programs on the Use of the Internet by Muslim-Americans, 7 Univ. of Maryland L. J. of Race, Religion, Gender (2007), 375, 391.

[98] Siehe oben Kapitel 3,A.II.1.

[99] Siehe oben Kapitel 3,A.II.2.b).

[100] *Schwabenbauer*, Heimliche Grundrechtseingriffe, 2013, 120.

[101] *Cohen*, Examined Lives, 52 Stanford L. Rev. Online (2000), 1373, 1425.

[102] *Seubert*, Der gesellschaftliche Wert des Privaten, DuD 2012, 100, 104; vgl.: *Schulhofer*, More Essential Than Ever, 2012, 12 und *Trepte*, Privatsphäre aus psychologischer Sicht, in: Schmidt/Weichert (Hrsg.), Datenschutz, 2012, 59, 63.

de nach und finden eigene Vorlieben und Erklärungen für auftauchende Fragen. Durch Ausprobieren verschiedener Optionen entwickeln sich Persönlichkeit und Ideen, die privates und geschäftliches Verhalten leiten. Dieser Prozess verlangt nicht nur nach umfassenden Informationen, sondern auch danach, neben gängigen gesellschaftlichen Weisheiten auch neue, als abwegig erachtete, kontroverse oder sogar anstößige Ansichten in Betracht zu ziehen. Er geht einher mit Fehlern, Meinungsumschwüngen und Neujustierungen der Überzeugung. Erst nach Erwägen einer Bandbreite an Optionen können Individuen die für sie persönlich richtige finden. Ihre Gedanken müssen Varianten berücksichtigen können, die sich außerhalb des gesellschaftlichen Mainstreams bewegen. Der Prozess muss Fehler und Meinungsänderungen zulassen, wollen die Individuen das für sie beste Ergebnis erzielen. Die dafür erforderliche Abgeschiedenheit kann bezeichnet werden als Freiraum der Individuen, um ihre Persönlichkeit aufblühen zu lassen.[103]

Darüber hinaus bedarf die Entwicklung neuer Ideen der Möglichkeit, vorläufige Ideen mit Vertrauten diskutieren und sie einer kleinen, selbstbestimmten Gruppe darlegen zu können.[104] So werden Feinheiten herausgearbeitet und Hypothesen getestet, ohne dass die Einzelnen sich schon zu der neu entstehenden These als ihrer festen, unabänderlichen Überzeugung bekennen müssten. Dieser Schritt ist essenziell, bietet er den Betroffenen doch die Chance, ihre Gedanken auszufeilen und mit relativ geringem Risiko des Ansehensverlustes Rückmeldung zu erlangen. Die Rede ist von einem „'infant industries' rationale, serving to nurture and shield new ideas from social disapproval before they are ready to be disclosed."[105] Je kontroverser die Idee, desto mehr werden die Individuen darauf angewiesen sein, sich von einem Irrweg abbringen zu lassen oder Bestätigung zu erfahren. Das Wechselspiel zwischen Denk- und Austauschprozess findet statt, bis die Einzelnen zu einem Ergebnis gelangen. Nach Abschluss der letzten Testphase kann die Idee verworfen oder dem weiteren Umfeld als eigene Vorstellung präsentiert werden.

Fraglich ist nun, wie sich Internetüberwachung auf den Denkprozess mit seinen beiden beschriebenen notwendigen Elementen – Freiheit des Denkvorgangs und Möglichkeit zur ungehinderten Diskussion – auswirkt. Denkprozess und Austausch mit Vertrauten finden in hohem Maße mediatisiert durch Online-Dienste statt.[106] Dokumente werden bei Cloud-Providern abgelegt, Gedankengänge in Internettagebüchern protokolliert, Ideen über E-Mails, Chat-Programme oder Foren ausgetauscht. Auch sind die Eingabe von Suchbegriffen in Suchmaschinen sowie das Aufrufen von Webseiten Ausdruck des stattfindenden Erkenntnisprozesses. Es wird zutreffenderweise darauf hingewiesen, dass es sich bei Suchanfragen um die intimsten und spontansten Online-Aktivitäten handeln kann, da sie unverblümte Ge-

---

[103] *Solove*, "I've Got Nothing to Hide" and Other Misunderstandings of Privacy, 44 San Diego L. Rev. (2007), 745, 762.

[104] So auch: *Schwabenbauer*, Heimliche Grundrechtseingriffe, 2013, 121.

[105] *Richards*, Intellectual Privacy, 87 Texas L. Rev. (2008), 387, 404.

[106] So auch: *Richards*, Intellectual Privacy, 87 Texas L. Rev. (2008), 387, 434; 444.

danken und Grübeleien reflektieren.[107] „Curiosity is monitored, producing a searchable database of the curious. […] Before search engines, no one had any records of curiosity; there was no list of questions asked.“[108] So dient das Internet nicht nur der Äußerung bereits gefasster Ideen, sondern gerade auch dem Denkvorgang als solchem. Die Rede ist von einer „migration of thought […] to the electronic environment“.[109]

Entsteht das Gefühl des Überwachtwerdens während des Denk- oder Kommunikationsprozesses, werden die Nutzer bei der Ausarbeitung ihrer Ideen stark eingeschränkt.[110] Ihre Gedankengänge werden durch die Manipulation ihrer Autonomie korrumpiert: „perfected surveillance of naked thought's digital expression short-circuits the individual's own process of decisionmaking.“[111] Um negative Folgen zu verhindern, kann es passieren, dass die Nutzer ihr Spektrum an möglichen Überzeugungen von vornherein auf die gesellschaftliche Norm beschränken und Extreme außer Acht lassen.[112] Kann ihnen jeder anfängliche Fehler später zum Nachteil gereichen, werden sie sich möglicherweise auf schon Anerkanntes reduzieren.[113] Es kann ein Verlust der Integrität individueller Gedankenfreiheit folgen.[114]

Zudem besteht die Gefahr, dass vorläufige Ideen nicht mit Vertrauten geteilt werden, um diesen negative Folgen zu ersparen. So befürchtete *Podlech* schon 1979 im Offline-Kontext: „Wer den Verdacht hegt, daß sein Briefwechsel kontrolliert oder sein Fernsprechverkehr abgehört wird, kann nicht mehr mit Freunden verkehren, um sie nicht einem Verdacht auszusetzen.“[115] Angesichts der vielfältigen Möglichkeiten der Aufzeichnung von Internetverhalten besitzt diese Furcht im Internetkontext mehr denn je Gültigkeit.

Um zu gewährleisten, dass auch Experimente mit neuen, kontroversen oder von der Norm abweichenden Ideen möglich sind, postuliert *Richards* daher den Schutz intellektueller Privatheit: „intellectual privacy – the protection of records of our intellectual activities […] safeguards the integrity of our intellectual activities by shielding them from the unwanted gaze or interference of others.“[116] Der Inhalt

[107] *Rubinstein/Lee/Schwartz*, Data Mining and Internet Profiling, 75 Chicago L. Rev. (2008), 261, 272.

[108] *Lessig*, Code, 2006, 204.

[109] *Richards*, Intellectual Privacy, 87 Texas L. Rev. (2008), 387, 444.

[110] So auch: *Schwartz*, Privacy and Democracy in Cyberspace, 52 Vanderbilt L. Rev. (1999), 1607, 1657.

[111] *Schwartz*, Privacy and Democracy in Cyberspace, 52 Vanderbilt L. Rev. (1999), 1607, 1656.

[112] So auch: *Cohen*, Examined Lives, 52 Stanford L. Rev. Online (2000), 1373, 1425 f.; *dies.*, DRM and Privacy, 18 Berkeley Tech. L. J. (2003), 575, 577; *Mitrou*, The impact of communications data retention on fundamental rights and democracy, in: Haggerty/Samatas (Hrsg.), Surveillance and Democracy, 2010, 127, 133 und *Richards*, Intellectual Privacy, 87 Texas L. Rev. (2008), 387, 425.

[113] So auch: *Gavison*, Privacy and the Limits of Law, 89 Yale L. J. (1980), 421, 448.

[114] *Richards*, Intellectual Privacy, 87 Texas L. Rev. (2008), 387, 389.

[115] *Podlech*, Das Recht auf Privatheit, in: Perels (Hrsg.), Grundrechte als Fundament der Demokratie, 1979, 50, 62.

[116] *Richards*, Intellectual Privacy, 87 Texas L. Rev. (2008), 387; vgl.: *ders.*, The Dangers of

dieser intellektuellen Privatheit wird anderorts beschrieben als „the extent of 'breathing space,' both metaphorical and physical, available for intellectual activity."[117] Die US-amerikanischen Verfechter der intellektuellen Privatheit bezwecken mit ihren Ausführungen primär die Einführung eines – dort weitgehend nicht existenten[118] – Schutzes der Internetaktivitäten der Bürger. Angesichts der gleichartigen Bedrohungen für die Gedankenfreiheit sind die Überlegungen jedoch auch auf den deutschen Kontext übertragbar.

Die Situation einer Gesellschaft, in der nicht nur normwidrige Äußerungen oder Verhaltensweisen, sondern schon bloße abseitige Gedankengänge beobachtet und sanktioniert werden, veranschaulicht der von *Orwell* in „Nineteen Eighty-Four" entwickelte Tatbestand „thoughtcrime", welcher beschrieben wird als „the essential crime that contained all others in itself."[119] Im Bestreben um absolute Kontrolle über ein einheitlich denkendes Volk kann das Regime jede Gefühlsregung als Notiz für abtrünnige Gedanken interpretieren und verfolgen. So soll bereits das Entstehen unliebsamer Ideen verhindert werden.

Aufzeichnungen über Denk- und Kommunikationsprozesse, die den Denkprozess protokollieren, bergen somit das Risiko, dass von der Norm abweichende Ideen nicht entstehen beziehungsweise ihnen nicht nachgegangen wird. Mainstream und unhinterfragter Konformismus werden bestärkt,[120] die Individuen langweilig.[121] Es folgt ein Verlust an Potenzial für kritisch-hinterfragende oder innovative Ideen.

Unter Anwendung dieser Überlegungen erscheint es plausibel, dass automatisierte Datenverarbeitung zu einer Selbstzensur auch hinsichtlich des Erkenntnisprozesses führt.

3. Zwischenfazit

Elektronische Aufzeichnungen intellektueller Aktivitäten und deren Auswertungen können in ihrer Wirkung mit konventioneller Überwachung vergleichbar sein und den individuellen Erkenntnisprozess beeinträchtigen. Dies kann geschehen, indem eine neutrale Quellenauswahl erschwert wird und die Preisgebenden Selbstzensur ausgesetzt sind. Selbstzensur kann dabei sowohl hinsichtlich der Quellenauswahl als auch der gefassten Ideen erfolgen.

Dies kann Auswirkungen auf die Persönlichkeitsentwicklung der Individuen haben:

Wird der Erkenntnisprozess durch Priorisierung von unter anderem auf das bisherige Rechercheverhalten der Nutzer zugeschnittenen Internetquellen gelenkt,

---

Surveillance, 126 Harvard L. Rev. (2013), 1934, 1945 ff. In diese Richtung geht auch schon: *Gavison*, Privacy and the Limits of Law, 89 Yale L.J. (1980), 421, 448 ff.

[117] *Cohen*, DRM and Privacy, 18 Berkeley Tech. L.J. (2003), 575, 576 f.; vgl.: 578.

[118] Siehe unten Kapitel 3,C.I.

[119] *Orwell*, Nineteen Eighty-Four, 1990 (Original: 1949), 14.

[120] So auch: *Cohen*, Examined Lives, 52 Stanford L. Rev. Online (2000), 1373, 1426.

[121] *Richards*, The Dangers of Surveillance, 126 Harvard L. Rev. (2013), 1934, 1948.

kann es zur verstärkten Wahrnehmung bestimmter Ansichten kommen. Wird er durch Selbst-Restriktion gestört, werden die individuellen Entfaltungschancen beeinträchtigt.[122]

Das daraus folgende Abstumpfen intellektueller Erkenntnisprozesse hin zu konformistischen Einheitsgedanken lässt die Persönlichkeit verarmen. Die Rede ist davon, dass ein Verlust informationeller Privatheit zu einer Gefahr wird für die „engine of expression – the imagination of the human mind".[123] Gedankenfreiheit kommt ein intrinsischer Wert als Ausübung individueller kognitiver Autonomie zu.[124] Schränken sich Individuen, wenn auch nicht bewusst, von vornherein im Prozess der Persönlichkeitsentwicklung ein und reduzieren Ideen, Ansichten und Interessen auf bisher Dagewesenes, bleiben ihnen eigene Erfolge und Erkenntnisse, die sie aus der Masse herausheben, verschlossen. Dadurch kann ihnen viel von dem, was zum eigenen Glück und Wohlbefinden beiträgt, entgehen.

Zudem kann informationelle Preisgabe mittelbar auch diverse andere Gefahren auslösen:

Unter einer fehlenden Möglichkeit zur Innovation leidet zunächst das individuelle Potenzial zu wirtschaftlichem Erfolg. Letzterer setzt häufig kreative Geschäftsmodelle abseits von Altbewährtem voraus. Diese werden durch das Unterdrücken von unabhängigen Gedanken und Entdeckungsgeist gebremst.

Zusammenfassend kommt es durch Manipulation der Quellenauswahl sowie Selbstzensur hinsichtlich der berücksichtigten Quellen und der gefassten Ideen zur Beeinträchtigung des intellektuellen Erkenntnisprozesses, wodurch die ein Leben lang andauernde Persönlichkeitsentwicklung sowie mittelbar auch vielfältige andere Interessen Schaden nehmen können.

III. Gefahren für Dritte und die Allgemeinheit

Der Übergang zwischen Gefahren für Rechte Dritter und für abstrakte Allgemeinwohlbelange scheint fließend. Nach einer Ansicht stellen Allgemeinwohlbelange nicht etwa eine „Summerierung von Einzelinteressen" dar, sondern sind ihnen gegenüber ein „aliud".[125] Nach anderer Ansicht kann von einer Unterscheidung abgesehen werden, da die Rechte der Allgemeinheit den Rechten oder Interessen anderer Menschen entspringen müssten.[126]

Das Bundesverfassungsgericht verzichtet auf eine seinen Grundrechtsprüfungen vorangestellte Differenzierung, wenn es in ständiger Rechtsprechung nur unterteilt in die beiden Kategorien der „dem Einzelnen oder der Allgemeinheit drohenden

---

[122] Vgl.: BVerfGE 65, 1 (43).
[123] *Richards*, Intellectual Privacy, 87 Texas L. Rev. (2008), 387, 404.
[124] *Richards*, Intellectual Privacy, 87 Texas L. Rev. (2008), 387, 405.
[125] *Häberle*, Die Wesensgehaltgarantie des Artikel 19 Abs. 2 Grundgesetz, [3]1983, 21.
[126] *Fischer*, Die Zulässigkeit aufgedrängten staatlichen Schutzes vor Selbstschädigung, 1997, 204 f.

Gefahren“[127] und feststellt, dass Grundrechtseingriffe nur zulässig sind, wenn sie zum Schutz des „Gemeinwohls“[128] erfolgen. Erst hinsichtlich der Frage nach der Rechtfertigung im Einzelfall untersucht es dann, welches Interesse konkret betroffen ist.

Realiter bleibt diese Aufbaufrage ohne Konsequenzen. Zwischen den Rechten Dritter und abstrakten Allgemeinwohlbelangen besteht ein enger Zusammenhang, sodass sie grundsätzlich gemeinsam behandelt werden können. Der Übersichtlichkeit halber erscheint es sachgerecht, der Terminologie des Bundesverfassungsgerichts zu folgen und erst kontextbezogen zu differenzieren. Soweit sich jedoch Abweichungen in der rechtlichen Beurteilung ergeben, ist eine Trennung vonnöten.

Die befürchteten Gefahren für das Allgemeinwohl könnten sich auf Dritte (siehe 1.), den gesellschaftlichen Fortschritt (siehe 2.) sowie auf das Gedeihen der Demokratie auswirken (siehe 3.).

1. Gefahren für Dritte

Informationelle Preisgabe könnte zu vielschichtigen Nachteilen für Dritte führen. Der Fokus wird im Folgenden auf denjenigen Bedrohungen liegen, die im direkten Zusammenhang mit den preisgegebenen Daten stehen. Solche Gefahren für Dritte könnten insbesondere entstehen aus dem aufgezwungenen Wissen über Andere sowie aus der Preisgabe von Daten, die auch Dritte betreffen. Demgegenüber bleibt die reine Verbreitung fremder Daten hier wie in der gesamten Arbeit außer Betracht.

Zunächst könnte es Dritten unangenehm sein, ohne ihren Willen Informationen über die Preisgebenden zu erhalten. Die eigene Entfaltung kann nicht nur dadurch beeinträchtigt werden, dass Andere zu viel über ein Individuum wissen. Vielmehr kann es lästig und mitunter die eigenen Verhaltensweisen prägend sein, ohne den eigenen Willen mit intimen Details Anderer konfrontiert zu werden. Viele gesellschaftliche Transaktionen verlangen nur nach sehr begrenzten Informationen über die Partner. Zusätzliches, für die Handlung an sich unerhebliches Wissen kann die Entscheidungen der Individuen beeinflussen. Es kann Vorurteile generieren, ein Bedürfnis zur Hilfeleistung auslösen oder die Individuen dazu veranlassen, ihre eigenen Wünsche hintanzustellen und mit an sich vorher unbeabsichtigter Preisgabe weiterer eigener Daten zu reagieren. Dadurch wird alltägliche Routine verkompliziert.[129] Auch wenn dieses aufgezwungene Wissen über Andere durchaus misslich sein kann, sind regelmäßig jedoch keine rechtlich geschützten Belange involviert. Der Aspekt kann daher für die weitere Analyse außer Acht bleiben.

---

[127] St. Rspr., statt vieler: BVerfGE 90, 145 (173).

[128] St. Rspr., statt vieler: BVerfGE 41, 360 (376); 81, 70 (84); 85, 248 (259) und 87, 363 (390); ausführlich zur „Gemeinwohljudikatur“ des Bundesverfassungsgerichts: *Fischer*, Die Zulässigkeit aufgedrängten staatlichen Schutzes vor Selbstschädigung, 1997, 114 ff.

[129] *Cohen*, Examined Lives, 52 Stanford L. Rev. Online (2000), 1373, 1427.

Relevant ist es hingegen, wenn aus preisgegebenen personenbezogenen Daten nicht nur Informationen über die Preisgebenden gewonnen werden können, sondern auch Rückschlüsse auf Dritte. Ein solcher mehrfacher Personenbezug der Daten wird häufig vorliegen. Dann stellt die Preisgabe eine Gefahr für die informationelle Privatheit dieser Dritten dar. Anschaulich werden die Rückschlussmöglichkeiten, die personenbezogene Daten auf die Identität Anderer geben, im Offline-Kontext am Beispiel von Zufallsfunden bei Massengentests, aus denen sich ergibt, dass der Täter wahrscheinlich mit einem der Teilnehmer der Untersuchung verwandt ist. Die Verwertung solcher sogenannten Beinahetreffer ohne ausdrückliche gesetzliche Grundlage ist grundsätzlich unzulässig, wie der Bundesgerichtshof 2012 entschied.[130]

Im Falle von im Internet preisgegebenen Daten ist beispielsweise zu denken an Fotografien, die auch Dritte abbilden oder an Statusmeldungen in sozialen Netzwerken, die beispielsweise auch persönliche Verhältnisse, Interessen, finanzielle Situation, Religionszugehörigkeit, politische Ausrichtung, Tätigkeit oder Aufenthaltsort Dritter offenlegen. In krassen Fällen kann das Bekanntwerden solcher Daten sogar dazu führen, dass die Dritten Opfer von Stalkingverhalten Anderer werden. Weiter werden, wenn sich Preisgebende entschließen, einen Teil ihrer genetischen Daten im Internet zu veröffentlichen, vielfältige Rückschlüsse auf ihre Verwandten ermöglicht.

Können auf Basis der Daten durch Big-Data-Analyse Erkenntnisse über Krankheiten, finanzielle Situation, politische Ausrichtung et cetera der jeweiligen Individuen erzielt werden, kann diesem Wissen unter Umständen Aussagekraft auch für Familienangehörige, Partner, Freunde, Nachbarn und Arbeitskollegen zukommen.

Betroffen sein können sogar Dritte, die in keinem irgendwie gearteten Näheverhältnis zu den Preisgebenden stehen, sondern sich etwa nur zeitgleich mit den Preisgebenden an einem Ort befanden, während diese Fotos aufnahmen und veröffentlichten.

Die Dritten haben regelmäßig keine Kontrolle über das Preisgabeverhalten der Nutzer. Informationelle Privatheit kann ihnen gegen ihren Willen und regelmäßig auch ohne ihre Kenntnis genommen werden. Informationelle Preisgabe kann daher die informationelle Privatheit Dritter gefährden.

2. Gefahren für die gesellschaftliche Entwicklung

Weiter könnten durch informationelle Preisgabe mittelbar Gefahren für den gesellschaftlichen Fortschritt in kultureller, wissenschaftlicher und auch wirtschaftlicher Hinsicht entstehen, die alle Bürger betreffen. Die Funktionsfähigkeit der Gesellschaft setzt individuelle Handlungskompetenz und Selbstbestimmung voraus.[131]

[130] BGH NJW 2013, 1827, 1829; siehe dazu BVerfG, Az. 2 BvR 616/13, Nichtannahmebeschluss vom 13.5.2015.

[131] *Simitis*, Selbstbestimmung, KJ 1988, 32.

Beide basieren auf dem Gelingen der individuellen intellektuellen Erkenntnisprozesse. Plastisch wird formuliert: „In order to speak, it is necessary to have something to say, and the development of ideas and beliefs often takes place best in solitary contemplation or collaboration with a few trusted confidants."[132] Die eingeschränkte Möglichkeit zu individuellem intellektuellem Erkenntnisprozess[133] schadet damit der Gesellschaft, deren Mitglieder weniger Interessantes beitragen können.[134] Durch eine Ausrichtung Einzelner hin zur vorgefertigten Meinung der Mehrheit kommt es zur Hemmung der freien Entwicklung der Bevölkerung. Es besteht die Gefahr des Entstehens von Gesellschaften, die geprägt sind durch Apathie und vorauseilenden Konformismus.[135] Freie Geister sind jedoch die Grundlage einer freien Gesellschaft.[136]

Voraussetzung kultureller Entwicklung ist das Hinterfragen von Bräuchen und Traditionen und entsprechend das Ablegen von Überkommenem. Es ist „wichtig, ungewöhnlichen Dingen einen möglichst freien Spielraum zu gewähren, damit es sich im Laufe der Zeit herausstellt, welche von ihnen sich dazu eignen, Tradition zu werden."[137] So können Missstände aufgedeckt werden und Veränderungsprozesse in Gang kommen. Grundlage wissenschaftlichen Erkenntnisgewinns sind Neugierde und Mut der Wissenschaftler, die offen für Neues ihrer Forschung nachgehen. Schließlich leistet die Ergänzung bestehender Geschäftsideen um neue, innovative Konzepte einen Beitrag zum Florieren der Wirtschaft. Niedrigere Kosten oder neue Produkte kommen den Käufern und Nutzern zugute, sodass die Innovation Einzelner zum Gemeinwohl beiträgt.[138]

Informationelle Preisgabe kann zu einer Behinderung der Persönlichkeitsentwicklung führen, indem die neutrale Quellenauswahl beeinträchtigt und der Selbstzensur hinsichtlich Quellenauswahl und Erkenntnisprozess Vorschub geleistet wird. Dadurch kann gesellschaftlicher Fortschritt auf verschiedene Weisen aufgehalten werden:

Kommt es durch personalisierte Quellenvorschläge zu einer Lenkung der Nutzer in eine bestimmte Richtung,[139] können sie dadurch von neuen, nicht zu ihrem bisherigen Profil passenden Ideen abgehalten werden.[140] Zudem kann gezielt die Entwicklung unliebsamer Ideen behindert werden. So erscheint es beispielsweise naheliegend, dass ein Internetumfeld, das Konsum und Gewinnmaximierung hinsicht-

---

[132] *Richards*, Intellectual Privacy, 87 Texas L. Rev. (2008), 387, 389.

[133] Siehe oben Kapitel 3,A.II.3.

[134] So auch: *Cohen*, What Privacy is For, 126 Harvard L. Rev. (2013), 1904, 1906; *Richards*, Intellectual Privacy, 87 Texas L. Rev. (2008), 387, 387; 405 und *ders.*, The Dangers of Surveillance, 126 Harvard L. Rev. (2013), 1934, 1948.

[135] *Cohen*, Examined Lives, 52 Stanford L. Rev. Online (2000), 1373, 1426f.

[136] *Richards*, The Dangers of Surveillance, 126 Harvard L. Rev. (2013), 1934, 1946.

[137] *Mill*, Über die Freiheit, 2010 (Original: 1859), 97.

[138] So auch: *Cooter/Ulen*, Law & Economics, [6]2010, 113.

[139] Siehe oben Kapitel 3,A.II.1.

[140] So auch: *Pariser*, Filter Bubble, 2012, 23.

lich angebotener Güter bezweckt, auf die Verhinderung von Ideen hinwirken wird, die gegenteiligen Zielen entsprächen.[141] Dadurch leidet die Überzeugungsfindung insgesamt.

Weiter geht mit vorauseilender Selbstzensur[142] hinsichtlich der Quellenauswahl und des Erkenntnisprozesses eine Beeinträchtigung der individuellen Fähigkeit einher, Bestehendes zu hinterfragen, Unzureichendes zu erkennen, eigene Gedanken zu fassen und neue Ideen abseits des Dagewesenen zu entwickeln. Eine solche individuelle Ideenlosigkeit kann in kultureller, wissenschaftlicher und wirtschaftlicher Hinsicht zu gesellschaftlicher Stagnation führen. Es kommt zu einer Bedrohung der Gesellschaft, in der kreative Individuen Erfindungen tätigen können und Unerwartetes produzieren.[143]

So kann individuelle informationelle Preisgabe im Wege der Beeinträchtigung der Quellenauswahl sowie der Selbstzensur hinsichtlich Quellenauswahl und Erkenntnisprozess den gesamtgesellschaftlichen Fortschritt hemmen.

3. Gefahren für eine funktionsgerechte Demokratie

Schließlich könnte ein Verlust informationeller Privatheit der Bürger die Demokratie insgesamt in Mitleidenschaft ziehen.

Die Funktionsfähigkeit einer Demokratie und die informationelle Privatheit ihrer Bürger bedingen sich gegenseitig. Einerseits sichern undemokratische Systeme ihren Machterhalt häufig durch Auflösung individueller informationeller Privatheit, wie Spitzelsysteme in diversen autoritären Regimes zeigen: Überwachung steht für Misstrauen gegenüber der eigenen Bevölkerung und gilt als Kennzeichen totalitärer Systeme.[144] Den Umfang solcher Informantensysteme verdeutlichen beispielsweise die 2013 auf der Enthüllungsplattform WikiLeaks veröffentlichten Details über Kontakte zwischen Herstellern elektronischer Überwachungstechnik und autoritären Regimes.[145] Andererseits zieht ein Verlust individueller informationeller Privatheit einen Schaden für die demokratische Gesellschaftsordnung nach sich. Dieser beruht darauf, dass jede Demokratie auf der politischen Teilnahme ihrer selbstbestimmten Bürger fußt,[146] jedoch deren Erkenntnismöglichkeit, Selbstbestimmtheit und Motivation zur politischen Teilnahme mit abnehmender informationeller Privatheit eingeschränkt werden. „Nur wer privat frei ist, kann politisch frei sein."[147]

---

141 So auch: *Cohen*, What Privacy is For, 126 Harvard L. Rev. (2013), 1904, 1927.

142 Siehe oben Kapitel 3,A.II.2.

143 So auch: *Schulhofer*, More Essential Than Ever, 2012, 178 f.

144 *Nagenborg*, Das Private unter den Rahmenbedingungen der IuK-Technologie, 2005, 129.

145 http://wikileaks.org/spyfiles3p.html.

146 So auch: *Häberle*, Die Wesensgehaltgarantie des Artikel 19 Abs. 2 Grundgesetz, [3]1983, 18, 20 und BVerfGE 65, 1 (43).

147 *Podlech*, Das Recht auf Privatheit, in: Perels (Hrsg.), Grundrechte als Fundament der Demokratie, 1979, 50, 53.

Demokratie zeichnet sich aus durch Mitwirkung der Bürger am Herrschaftsprozess. Das Volk ist souveräner Träger der Staatsgewalt, die Legitimation seiner Repräsentanten wird von ihm abgeleitet.[148] Voraussetzung für die Selbstbestimmung des Volkes ist die Selbstbestimmung seiner Mitglieder.[149] Um die Mitwirkung sinnvoll ausführen zu können, benötigen Bürger eine gewisse Befähigung. Diese „geistig-bildungsmäßigen Voraussetzungen“ sind ein „Grundbestand an Bildung und Wissen“, ein „darauf gegründete[s] eigene[s] Urteilsvermögen“ sowie die „Möglichkeit von Information und Kommunikation in der Gesellschaft“.[150] Informationelle Privatheit ist Grundlage für den individuellen intellektuellen Erkenntnisprozess, der alleine oder im Dialog mit ausgewählten Vertrauten erfolgt. So kann informationelle Privatheit als geistig-bildungsmäßige Voraussetzung angesehen werden, die der Demokratie zugrunde liegt.

Der Verlust informationeller Privatheit hingegen könnte, wie im Folgenden untersucht wird, die Bürger daran hindern, die Notwendigkeit von Veränderungen und deren Inhalt zu erkennen (siehe a)), ihrer Selbstbestimmtheit schaden (siehe b)) und sie von politischer Partizipation abschrecken (siehe c)). Dadurch könnte politische Teilnahme gefährdet werden.

a) Möglichkeit zum Erkennen notwendiger Veränderungen

Informationelle Preisgabe könnte darin resultieren, dass Bürger in ihrer Fähigkeit eingeschränkt werden, notwendige politische Veränderung zu erkennen.

Voraussetzung für politische Revisionen sind Akteure, die diese einleiten. So bedarf eine Demokratie des Einschreitens ihrer Bürger, wenn tatsächliche Lage und Überzeugungen der Bevölkerung divergieren. Ein solches Aktivwerden kann jedoch nur erfolgen, wenn die Einzelnen erkennen, dass die Realität von ihren Vorstellungen abweicht.

Wird der Erkundungsprozess der Bürger dadurch gestört, dass ihnen Informationen priorisiert entsprechend der eigenen Ansichten in sogenannten Filter Bubbles präsentiert werden,[151] kann die Überzeugung entstehen, Missstände bestünden nicht oder würden bereits von einer ausreichenden Anzahl anderer Bürger behoben, sodass ein eigenes Tätigwerden nicht notwendig erscheint. Auch können den Nutzern Informationen über Miseren verborgen bleiben, da Unangenehmes und Kompliziertes regelmäßig weniger gerne gelesen wird als Erfreuliches und Bekanntes.

---

[148] Vgl. für Deutschland: Art. 20 Abs. 2 GG.

[149] *Schneider*, Eigenart und Funktionen der Grundrechte im demokratischen Verfassungsstaat, in: Perels (Hrsg.), Grundrechte als Fundament der Demokratie, 1979, 11, 43; *Simitis*, Selbstbestimmung, KJ 1988, 32, 42 f. und *Starck*, Grundrechtliche und demokratische Freiheitsidee, in: Isensee/Kirchhof (Hrsg.), Handbuch des Staatsrechts der Bundesrepublik Deutschland III, 2005, 3 ff., Rn. 4.

[150] *Böckenförde*, Demokratie als Verfassungsprinzip, in: Isensee/Kirchhof (Hrsg.), Handbuch des Staatsrechts der Bundesrepublik Deutschland II, 2004, 429 ff., Rn. 67 f.

[151] Siehe oben Kapitel 3,A.II.1.

Was den Nutzern gefällt, muss nicht unbedingt dem entsprechen, was sie wissen sollten, um informierte Mitglieder eines Gemeinwesens oder Bürger eines Staates zu sein.[152] So wird in einer mit den Mitteln der Big-Data-Analyse modulierten Gesellschaft das individuelle „information environment" dem persönlichen „comfort level" angepasst; Motivation der Bürger, Verbesserungen anzugehen, erfordert jedoch ein „certain amount of *dis*comfort".[153] Informationelle Preisgabe, die dazu führt, dass die Nutzer vorrangig entsprechend ihren eigenen Vorstellungen mit Informationen versorgt werden, kann somit zu einem Verlust der Neigung zum Ergreifen von Veränderungen führen. Unter dieser Antriebslosigkeit leidet letztlich die Demokratie.[154]

b) Selbstbestimmte Bürger als Politik-Subjekte

Weiter könnte informationelle Preisgabe dazu führen, dass Bürger die Selbstbestimmtheit einbüßen, die notwendig wäre, um einen sinnvollen politischen Beitrag leisten zu können.

Pluralistische Meinungsbildung erfordert engagierte und politisch interessierte Bürger, die selbstbestimmt Überzeugungen bilden und diese in die öffentliche Diskussion einbringen.[155] Datenschutz ist „Funktionsbedingung eines demokratischen Gemeinwesens", Teilnahme an demokratischer Willensbildung ist nur zu erwarten, wenn jeder Teilnehmer sein Handeln auf freier Willensbildung gründen kann.[156] Die freie Willensentschließung lässt sich somit als Keimzelle jeder freiheitlichen Demokratie bezeichnen.[157] Nehmen Bürger ihre informationelle Selbstbestimmung nicht wahr, trifft dies „nicht nur die Idee eines gelungenen – selbstbestimmten – Lebens, sondern auch die Idee der liberalen Demokratie: die nämlich auf autonome und sich ihrer Autonomie bewusste und diese schätzende Subjekte angewiesen ist."[158]

Für das Gedeihen der Demokratie ist es grundlegend, dass Regierungshandeln kritisch hinterfragt und durch Wahlen, Abstimmungen oder den Druck der öffentlichen Meinung unterstützt oder zu Veränderungen bewegt wird. Verlieren Bürger

---

[152] So auch: *Pariser*, Filter Bubble, 2012, 26, 81 f.

[153] *Cohen*, What Privacy is For, 126 Harvard L. Rev. (2013), 1904, 1918 (Hervorhebung im Original).

[154] So auch: *Richards/King*, Three Paradoxes of Big Data, 66 Stanford L. Rev. Online (2013), 41, 44.

[155] *Regan*, Legislating Privacy, 1995, 225 ff.; *Richards*, Intellectual Privacy, 87 Texas L. Rev. (2008), 387, 391; *Schwabenbauer*, Heimliche Grundrechtseingriffe, 2013, 112 und *Schwartz*, Beyond Lessig's Code for Internet Privacy Wisconsin L. Rev. 2000, 743, 761 f.

[156] *Roßnagel/Pfitzmann/Garstka*, Modernisierung des Datenschutzrechts, 2001, 21; vgl. BVerfGE 65, 1 (43).

[157] *Schneider*, Eigenart und Funktionen der Grundrechte im demokratischen Verfassungsstaat, in: Perels (Hrsg.), Grundrechte als Fundament der Demokratie, 1979, 11, 43.

[158] *Rössler*, Der Wert des Privaten, 2001, 218; so auch: *Gavison*, Privacy and the Limits of Law, 89 Yale L. J. (1980), 421, 455.

durch Preisgabe ihrer informationellen Privatheit die Möglichkeit oder das Interesse, Bestehendes zu hinterfragen und Impulse zu geben,[159] schwindet auch ihre Fähigkeit, zum Gedeih der demokratischen Grundordnung beizutragen. Deutlich machen lässt sich dies, indem man eine Gesellschaftsordnung entwirft, in der zwar der Akt öffentlichen Sprechens geschützt ist, jedoch nicht der zugrunde liegende Erkenntnisprozess. In einem solchen System könnte zwar viel gesagt werden, aber dies kaum Neues bringen, da originelle Ideen keinen Schutzraum zur Entwicklung hätten.[160]

Eine Selbstbeschränkung des intellektuellen Erkenntnisprozesses lässt so die Fähigkeit schrumpfen, sinnvoll zur öffentlichen Debatte beizutragen. Diese Problematik wird auch als Verlust des Potenzials zur demokratischen „self-governance" bezeichnet. Ein solches ist nur gegeben bei Individuen, die imstande sind, ihre eigenen Überzeugungen zu formen und entsprechend zu handeln.[161] Soweit „self-governing communities" von dem psychologischen Wohl und der unabhängigen Entscheidungen ihrer Mitglieder profitieren, kommt Privatheit damit ein sozialer Wert zu.[162]

Entsteht hingegen durch informationelle Preisgabe und die daraus folgende Beeinträchtigung der Persönlichkeitsbildung der Individuen eine konturlose konformistische Bürgerschaft, schwindet deren Möglichkeit, einen selbstbestimmten Beitrag zum Gedeihen der Demokratie zu leisten.

c) Abschreckung von politischer Partizipation

Weiter könnte informationelle Preisgabe mittelbar die Preisgebenden und auch Dritte von politischer Teilnahme abschrecken und so die Demokratie beeinträchtigen.

Politische Teilnahme durch Bürger erfolgt im Wege von Wahlen und Abstimmungen, aber auch durch ihre Beiträge zum politischen Meinungsbildungsprozess. Dieser kann beispielsweise durch die Teilnahme an Demonstrationen, das Engagement in Parteien und Interessengruppen,[163] den öffentlichen Einsatz für oder gegen bestimmte Anliegen, Einträge in Internetforen oder durch Äußerungen im Rahmen kultureller Medien, wie Literatur, Zeitungen, Theater und Fernsehen geschehen. Der Beitrag kann unter Offenlegung der eigenen Person erfolgen oder im Bemühen, unerkannt zu bleiben.

Jedes Verhalten, das auf politische Überzeugungen schließen lässt, ist in hohem Maße sensibel. Die Einzelnen wissen nicht, ob ihnen politische Äußerungen später im privaten oder geschäftlichen Bereich schaden können. So ist ein Bias seitens privater Bekanntschaften, Geschäftspartner oder zukünftiger Arbeitgeber aufgrund

---

159 Siehe oben Kapitel 3,A.II.
160 *Richards*, Intellectual Privacy, 87 Texas L. Rev. (2008), 387, 403.
161 *Schwartz*, Privacy and Democracy in Cyberspace, 52 Vanderbilt L. Rev. (1999), 1607, 1647.
162 *Allen*, Privacy Law and Society, ^{2}2011, 8.
163 Zu diesen Aspekten, siehe bereits: BVerfGE 65, 1 (43).

politischer Äußerungen denkbar. Weiter können die Preisgebenden die Entwicklung der politischen Lage nicht vorhersehen, sodass ihnen frühere politische Bekundungen später zum Nachteil gereichen können. Schließlich besteht die Möglichkeit, dass die Preisgebenden selbst ihre politische Meinung revidieren und, um bei der Kundgabe der neu gefundenen Überzeugung glaubhaft erscheinen zu können, nicht mit vergangenen Äußerungen in Bezug gebracht werden möchten.

Vor diesem Hintergrund erscheint es naheliegend, dass den Preisgebenden Internetaufzeichnungen, die ihre politische Teilnahme mit ihnen in Zusammenhang setzen, unangenehm werden können. Solche Aufzeichnungen können auf zweierlei Weise entstehen: Zunächst durch politische Partizipation im Internetkontext, beispielsweise durch Blog-Einträge, Online-Petitionen oder E-Mail-Kommunikation. Darüber hinaus können jedoch auch Offline-Äußerungen mit den Nutzern verbunden werden, wenn ein Abgleich mit anderweitig online preisgegebenen personenbezogenen Daten eine Identifizierung ermöglicht. Zu denken ist beispielsweise an Überwachungskameras mit Gesichtserkennungsfunktion oder Berichterstattungen, die etwa Gesichter von Demonstranten oder Theaterzuschauern erfassen und mittels automatisierter Gesichtserkennung zur Identifizierung der Individuen führen können,[164] soweit als Folge vorangegangener Preisgabe entsprechende Datensätze vorhanden sind. Je mehr personenbezogene Daten Dritten bekannt und insbesondere in Datenbanken eingearbeitet sind, desto höher ist die Chance, dass auch Offline-Verhalten mit den Einzelnen in Verbindung gebracht werden kann. Darüber hinaus resultiert der Trend zur allgegenwärtigen Datenverarbeitung (sogenanntes Ubiquitous Computing) darin, dass eine steigende Anzahl an realen Handlungen Datenspuren hinterlässt.[165] Informationelle Preisgabe führt so dazu, dass den Nutzern politisches Verhalten innerhalb und außerhalb des Internets direkt oder auf Umwegen zuordenbar sein kann.

Soweit die Nutzer nicht bereit sind, sich schon jetzt zu ihren politischen Ansichten auch in ferner Zukunft und unabhängig von potenziellen, noch nicht absehbaren negativen Konsequenzen, zu bekennen, besteht daher die Möglichkeit, dass sie von vornherein ihre Handlungsweisen zur Vermeidung dieser Auswirkungen auf die vermeintliche gesellschaftliche Norm limitieren.[166] Angesichts des technischen Fortschritts und der Unabsehbarkeit der Konsequenzen, die politische Teilnahme haben kann, steht zu befürchten, dass Nutzer ihre politischen Aktivitäten auf Dauer entweder einstellen, reduzieren oder auf den Mainstream beschränken, um Nachteile zu vermeiden. Nur begrenzt weiterführend ist daher der Hinweis, die wahren

---

[164] So scannt angeblich die US-National Security Agency die täglich abgefangenen Millionen Bilder und vergleicht sie mit in ihren Datenbanken hinterlegten Bildern, *DANA Redaktion*, NSA scannt Netz nach Gesichtern, DANA 2014, 122 ff.

[165] Hierzu umfassend: *Roßnagel*, Datenschutz in einem informatisierten Alltag, 2007.

[166] *Seubert*, Der gesellschaftliche Wert des Privaten, DuD 2012, 100, 104; *Solove*, Nothing to Hide, 2011, 178 f.; *Schulhofer*, More Essential Than Ever, 2012, 13, 179 und *Schwabenbauer*, Heimliche Grundrechtseingriffe, 2013, 112; siehe oben Kapitel 3,A.II.2.

Helden unserer Gesellschaft seien gerade diejenigen, die in Kenntnis der Risiken gegen Autoritäten protestieren.[167] Dem Umstand, dass trotz langfristigen Verlusts informationeller Privatheit politische Teilnahme existieren kann, kommt keine Aussagekraft darüber zu, wie viel intensiver die politische Teilnahme bei der Existenz voller informationeller Privatheit ausgefallen wäre.

Die Auswirkungen, die das Gefühl von Ausforschung auf Journalisten als wichtige Akteure in einer Demokratie haben kann, zeigt die bereits erwähnte Befragung von 528 US-amerikanischen Journalisten im Jahr 2013. Demnach haben aus Angst vor Überwachung 28 Prozent die Nutzung sozialer Netzwerke eingeschränkt oder vermieden, 12 Prozent haben dies ernsthaft erwogen. Weiter haben 16 Prozent es gemieden, über bestimmte Themen zu sprechen, 11 Prozent haben dies ernsthaft in Betracht gezogen.[168]

Eine Demokratie erfordert Menschen, die ihre Meinung äußern und anderen zuhören – „But who will speak or listen when this behavior leaves finely-grained data trails in a fashion that is difficult to understand or anticipate?“[169] Die demnach zu erwartenden Einschüchterungseffekte schaden der Gesellschaft, indem sie die Bandbreite an vertretenen Ansichten und das Maß an Freiheit, sich politisch zu engagieren, vermindern.[170]

Die Auswirkungen solcher Einschüchterungseffekte könnten dadurch verstärkt werden, dass es sich bei politischer Teilnahme um einen fragilen Prozess handelt.[171] Sie kostet die Einzelnen den Aufwand der Recherche, Entscheidungsfindung und Ausführung der politischen Teilnahme. Als Nutzen können die Parteien an die Macht gelangen beziehungsweise die Initiativen gestärkt werden, die den individuellen Interessen am nächsten kommen. Schon hier ist fraglich, wie sehr sich die Wahl der politischen Machthaber tatsächlich auf die Interessen der Einzelnen auswirkt. Doch dies kann im Regelfall dahingestellt bleiben, da die einzelnen Stimmen bei einer Wahl oder die individuellen Teilnehmer einer Demonstration ein vernach-

---

[167] *Bull*, Zweifelsfragen um die informationelle Selbstbestimmung, NJW 2006, 1617, 1623.

[168] *FDR Group*, The Impact of US Government Surveillance on Writers, 31.10.2013; siehe oben Kapitel 3,A.II.2.b).

[169] *Schwartz*, Privacy and Democracy in Cyberspace, 52 Vanderbilt L. Rev. (1999), 1607, 1651.

[170] So auch: *Mitrou*, The impact of communications data retention on fundamental rights and democracy, in: Haggerty/Samatas (Hrsg.), Surveillance and Democracy, 2010, 127, 133 und *Solove*, “I’ve Got Nothing to Hide” and Other Misunderstandings of Privacy, 44 San Diego L. Rev. (2007), 745, 765.

[171] Dass trotz geringen Eigennutzes Millionen von Menschen politisch aktiv sind (sei es auch nur dadurch, dass sie an Wahlen teilnehmen), kann zunächst Verwunderung auslösen. Dieses sogenannte Paradox des Wählens wurde zuerst von *Downs* beschrieben: „Thus, when benefits are indivisible, each individual is always motivated to evade his share of the costs of producing them. If he assumes that the behavior of others is given, whether or not he receives any benefits does not depend on this own efforts. But the cost he pays does depend on his efforts; hence the most rational course for him is to minimize that cost – in this case, to remain politically ignorant.“: *Downs*, An Economic Theory of Political Action in a Democracy, 65 J. of Political Economy (1957), 135, 147. Dem ist jedoch entgegen zu halten, dass auch altruistisches Verhalten rational sein kann, wenn die Betroffenen ein Interesse am Erhalt des Gemeinwohls haben.

lässigbar kleines Gewicht im Verhältnis zum Gesamtprozess haben. Sie kosten diese selbst Mühen, führen jedoch einzeln betrachtet in aller Regel zu keiner messbaren Veränderung.[172] Diese Erkenntnis kann eine Ermüdung der Wähler herbeiführen und diese dazu bewegen, entweder gänzlich auf politische Beteiligung zu verzichten oder den erforderlichen Aufwand auf ein Mindestmaß zu kürzen. So ist es aus Sicht der einzelnen Individuen nicht abwegig, keine Ressourcen zum Hinterfragen bestehender politischer Ansichten zu verwenden. Dies führt zum Entstehen des sogenannten Trittbrettfahrerproblems, da die politisch Nichtaktiven vom Einsatz derjenigen profitieren, die durch beständiges Hinterfragen die Demokratie am Leben erhalten. Der Mangel an positiven Anreizen zur politischen Teilnahme macht den Prozess besonders anfällig für Kräfte wie die Angst vor späteren negativen Konsequenzen, die die Teilnahme verhindern möchten.

Informationelle Preisgabe kann daher dazu führen, dass Bürger von politischer Teilnahme abgeschreckt werden. Darunter leidet die Demokratie, die die Mitwirkung ihrer Bürger zur Funktionsbedingung hat.

IV. Zwischenfazit

Die Preisgabe personenbezogener Daten im Internet kann zu einer Einschränkung des für die individuelle Persönlichkeitsentwicklung essenziellen intellektuellen Erkenntnisprozesses führen.

In deren Folge drohen Gefahren für die Allgemeinheit in Gestalt von Gefahren für konkrete Dritte, den gesellschaftlichen Fortschritt sowie das Gedeihen der Demokratie. Zunächst können aus preisgegebenen Daten Gefahren für die informationelle Privatheit Dritter entstehen. Weiter kann informationelle Preisgabe im Wege der Beeinträchtigung der Quellenauswahl sowie der Selbstzensur hinsichtlich der Quellenauswahl und des Erkenntnisprozesses auch den gesamtgesellschaftlichen Fortschritt hemmen. Schließlich kann die Demokratie gefährdet werden, da ihre Bürger die Fähigkeit zum Erkennen notwendiger Veränderungen verlieren können, es ihnen an der erforderlichen Selbstbestimmung fehlen kann und sie schließlich von politischer Teilnahme abgeschreckt werden können. Darunter leidet die Demokratie, die die Mitwirkung ihrer Bürger zur Funktionsbedingung hat.

B. Gefährdete Rechtsgüter nach dem Grundgesetz

Sowohl hinsichtlich einer Pflicht[173] des Staates zur Verhinderung informationeller Preisgabe als auch hinsichtlich einer entsprechenden Befugnis[174] ist ausschlaggebend, auf welche Rechtsgüter sich die tatsächlichen Gefahren auswirken können

---

[172] *Posner*, Economic Analysis of Law, [7]2007, 564.
[173] Siehe unten Kapitel 5,A.
[174] Siehe unten Kapitel 6,A.

und in welcher Weise das Grundgesetz die durch die Preisgabe bedrohten Rechtsgüter schützt. Je wichtiger die Verfassung die bedrohten Belange nimmt, desto größer ist auch das verfassungsrechtliche Interesse an der Verhinderung informationeller Preisgabe, die diese Belange gefährdet.

Es ist daher zu untersuchen, ob die abstrakt[175] bedrohten Belange der Preisgebenden (siehe I) und der Allgemeinheit (siehe II) verfassungsrechtlich geschützte Interessen darstellen.

I. Rechtsgüter der Preisgebenden

Zunächst ist nach den durch Dritte mittelbar[176] bedrohten Rechtsgütern der Preisgebenden zu fragen.

Informationelle Preisgabe kann dazu führen, dass Nutzer auf lange Sicht gesehen die Möglichkeit verlieren, selbst zu entscheiden, wann und innerhalb welcher Grenzen persönliche Sachverhalte offenbart werden sollen und in der Folge Selbstzensur üben. Ein solcher Kontrollverlust könnte insbesondere[177] durch das Recht auf informationelle Selbstbestimmung geschützte Interessen berühren (siehe 1.).

Weiter können Nutzer durch informationelle Preisgabe an neutraler Quellenauswahl gehindert werden oder aus vorauseilendem Gehorsam von der Nutzung kontroverser Quellen absehen. Durch einen solchen gehinderten Zugang zu Informationen könnten durch die Informationsfreiheit geschützte Interessen berührt werden (siehe 2.).

1. Recht auf informationelle Selbstbestimmung

Wenn Nutzer nicht mehr abschätzen können, wann und innerhalb welcher Grenzen sie betreffende persönliche Sachverhalte offenbart sind, kann dies zu einer Selbstzensur sowohl hinsichtlich der Quellenauswahl[178] als auch hinsichtlich des Erkenntnisprozesses führen.[179] Dadurch könnten Interessen bedroht werden, die durch das Recht auf informationelle Selbstbestimmung geschützt sind.

---

[175] Die Arbeit widmet sich der abstrakten Gefahrenanalyse, ohne im Einzelnen jede denkbare konkrete Gefährdung zu beleuchten.

[176] Auf tatsächlicher Ebene wird zunächst herausgearbeitet, welche Interessen durch Verhalten Privater bedroht werden können. Da diese Privaten selbst nicht an Grundrechte gebunden sind, wird sodann unter Kapitel 5,A und Kapitel 6,A untersucht, ob der Staat zum Schutz der Nutzerinteressen eingreifen muss beziehungsweise darf.

[177] Je nach Kontext können auch weitere Grundrechte betroffen sein, etwa die Meinungs- oder Versammlungs- oder Vereinigungsfreiheit, vgl. BVerfGE 65, 1 (43). Häufig wird die Bedrohung dieser Grundrechte jedoch Folgewirkung des Verlusts der informationellen Selbstbestimmung sein, sodass sich die Analyse auf Letzteren beschränkt.

[178] Siehe oben Kapitel 3,A.II.2.b).

[179] Siehe oben Kapitel 3,A.II.2.c).

a) Funktion und Schutzbereich

Aus dem Wortlaut des Grundgesetzes folgt das Recht auf informationelle Selbstbestimmung nicht ausdrücklich. Politische Bestrebungen[180] zur Einführung eines solchen Grundrechts sind bislang ohne Erfolg geblieben. Zu nennen ist beispielhaft die gescheiterte Verfassungsnovelle von Bündnis 90/Die Grünen aus dem Jahr 2008. Diese bezweckte unter anderem die Einführung eines Art. 2a GG: „Das Recht, über persönliche Daten selbst zu bestimmen, wird gewährleistet. Beschränkungen dieses Rechtes bedürfen einer gesetzlichen Grundlage.“[181]

Dem allgemeinen Persönlichkeitsrecht (Art. 2 Abs. 1 in Verbindung mit Art. 1 Abs. 1 GG) wurde bereits recht früh ein Schutzanspruch der Einzelnen gegen zu viel staatliche Kenntnisnahme persönlicher Sachverhalte entnommen.[182] Erinnert sei an den Mikrozenus-Beschluss des Bundesverfassungsgerichts, nach dem es verfassungswidrig ist, „den Menschen zwangsweise in seiner ganzen Persönlichkeit zu registrieren und zu katalogisieren“.[183] Ähnliche Ansätze finden sich auch in den Entscheidungen zu Ehescheidungsakten,[184] zur ärztlichen Schweigepflicht,[185] zur Dokumentation über den Soldatenmord in Lebach[186] sowie zu der Durchsuchung einer Drogenberatungsstelle.[187] Auch in der datenschutzrechtlichen Literatur wurden bereits früh Rufe nach dem Schutz eines Rechts auf informationelle Selbstbestimmung laut.[188]

Erheblich ausgeweitet wurde der skizzierte Schutz dann im sogenannten Volkszählungsurteil des Bundesverfassungsgerichts aus dem Jahr 1983,[189] mit dem es

---

180 Die Diskussion nachzeichnend: *Künast*, „Meine Daten gehören mir” – und der Datenschutz gehört ins Grundgesetz, ZRP 2008, 201, 202 ff.; *Kutscha*, Mehr Datenschutz – aber wie?, ZRP 2010, 112, 114; *Roßnagel/Pfitzmann/Garstka*, Modernisierung des Datenschutzrechts DuD 2001, 253, 256 und *Schliesky/Hoffmann/Luch u. a.*, Schutzpflichten und Drittwirkung im Internet, 2014, 149 ff.; ablehnend: *Bull*, Informationelle Selbstbestimmung, 2009, 119 ff; zur Funktion einer Kodifizierung richterrechtlicher „Grundrechtsinnovationen“: *Hornung*, Grundrechtsinnovationen, 2015.

181 Entwurf eines Gesetzes zur Änderung des Grundgesetzes, BT-Drs. 16/9607 v. 18.6.2008.

182 Zur Bedeutung des allgemeinen Persönlichkeitsrechts für den grundgesetzlichen Privatheitsschutz: *Stern*, Der allgemeine Privatsphärenschutz durch das Grundgesetz und seine Parallelen im internationalen und europäischen Recht, in: Bröhmer/Bieber/Calliess u. a. (Hrsg.), Internationale Gemeinschaft und Menschenrechte, 2005, 1259, 1261.

183 BVerfGE 27, 1 (6).

184 BVerfGE 27, 344 (354 ff.).

185 BVerfGE 32, 373 (378 ff.).

186 BVerfGE 35, 202 (220 ff.).

187 BVerfGE 44, 353 (372 f.).

188 *Podlech*, Verfassungsrechtliche Probleme öffentlicher Informationssysteme, 1 DVR (1972/73), 149 ff.; *ders.*, Das Recht auf Privatheit, in: Perels (Hrsg.), Grundrechte als Fundament der Demokratie, 1979, 50, 55 ff. und *Steinmüller/Lutterbeck/Mallmann u. a.*, Grundfragen des Datenschutzes, 7.1971, 84 ff.; die Entwicklung nachvollziehend: *Amelung*, Der Schutz der Privatheit im Zivilrecht, 2002, 39 ff.

189 Zu den folgenden Ausführungen, soweit nicht anders angegeben: BVerfGE 65, 1 (42 ff.). Eine englischsprachige Übersetzung findet sich in: Federal Constitutional Court Human Rights L. J., 51984, 94 ff.; zur Innovationsgeschichte des Rechts auf informationelle Selbstbestimmung:

auf entstehende technische Privatheitsbedrohungen reagierte und das Recht auf informationelle Selbstbestimmung aus dem entwicklungsoffenen allgemeinen Persönlichkeitsrecht und dem dadurch geschützten Recht auf Selbstdarstellung ableitete.[190]

Moderne Informationstechnologien bergen das Risiko, dass durch automatisierte Datensammlung und -verarbeitung umfassende Erkenntnisse über die Bürger gewonnen werden, mithin eine totale Registrierung und Katalogisierung stattfindet. Dadurch steht die Gefahr im Raum, dass die Individuen ihre Subjektsqualität verlieren und zum bloßen Objekt von systematischen Datensammlungen und Datenverarbeitungsprozessen werden. Diese Bedrohung ruft die Schutzgewähr der durch Art. 1 Abs. 1 GG geschützten Menschenwürde auf den Plan. Diese verbietet die Behandlung der Grundrechtsträger als bloßes Objekt. Das Gericht anerkennt den hohen Wert der Entscheidungs- und Handlungsfreiheit als Voraussetzung individueller Selbstbestimmung. Selbstbestimmte Teilnahme am Kommunikationsprozess ist Voraussetzung für die freie Entfaltung der Persönlichkeit.[191] Diese Freiheit ist bedingt durch die Transparenz der Informationszusammenhänge, also durch die Möglichkeit der Einzelnen, überschauen zu können, welche sie betreffenden Informationen in bestimmten Bereichen ihrer sozialen Umwelt bekannt sind, sowie das Wissen möglicher Kommunikationspartner einigermaßen abschätzen zu können.[192] Um diese Transparenz zu wahren, verbietet das Recht auf informationelle Selbstbestimmung das Entstehen einer Rechtsordnung, in der die Bürger nicht mehr wissen können, „wer was wann und bei welcher Gelegenheit über sie weiß".[193] Diese Forderung ist freilich nicht wörtlich zu nehmen, da Demokratie und freier Markt des informierten Diskurses bedürfen.[194] Vielmehr gewährleistet das Recht auf informationelle Selbstbestimmung den Schutz der Einzelnen gegen eine unbegrenzte Erhebung, Speicherung, Verwendung und Weitergabe ihrer personenbezogenen Daten.[195] Die Daten dürfen insbesondere nur für den Zweck verarbeitet oder verwendet werden, für den sie erhoben oder gespeichert wurden.[196] Angesichts unabsehbarer technischer Möglichkeiten bedürfen sensible, gleich wie auf den ersten Blick unsensible, personenbezogene Daten jedenfalls grundsätzlich des Schutzes, es gibt „kein belangloses Datum mehr".[197] Die Transparenz der Informationszusammenhänge ist

Hornung, Grundrechtsinnovationen, 2015, 266 ff.; zu den gesellschaftlichen und juristischen Hintergründen: *Frohmann*, Only Sheep Let Themselves Be Counted, in: Friedrich-Ebert-Stiftung (Hrsg.), Archiv für Sozialgeschichte, 2012, 335, 342 ff. und *Simitis*, in: ders. (Hrsg.), Bundesdatenschutzgesetz, 2014, Einleitung, Rn. 27 ff.

[190] Vgl. Maunz/Dürig-GG/*Di Fabio*, 2014, Art. 2, Rn. 175.

[191] Siehe oben Kapitel 3,A.II.3.

[192] BVerfGE 65, 1 (43).

[193] BVerfGE 65, 1 (43).

[194] *Masing*, Herausforderungen des Datenschutzes, NJW 2012, 2305, 2307.

[195] BVerfGE 65, 1 (43).

[196] BVerfGE 65, 1 (46); ausführlich: *Zezschwitz*, Konzepte der normativen Zweckbegrenzung, in: Roßnagel (Hrsg.), Handbuch Datenschutzrecht, 2003, 219, 221 ff., Rn. 1 ff.

[197] BVerfGE 65, 1 (45).

dabei nicht Selbstzweck, sondern lediglich Mittel zum Schutz der informationellen Selbstbestimmung.

Die Ableitung des Rechts auf informationelle Selbstbestimmung aus dem allgemeinen Persönlichkeitsrecht sowie seine inhaltliche Ausgestaltung durch das Bundesverfassungsgericht haben in der Literatur damals wie heute überwiegend Zustimmung gefunden.[198]

Nach *Starck* stellt die Bezeichnung Recht auf informationelle Selbstbestimmung eine „wenig glückliche" Umschreibung eines Aspekts des Art. 2 Abs. 1 GG dar, „ohne dass dem neuen Wort irgendeine grundrechtssteigernde oder tatbestandspräzisierende Bedeutung zukäme."[199] Diese Kritik findet jedoch zurecht wenig Zuspruch. Die Bezeichnung erweist sich inhaltlich als treffend, denn das Schutzgut ist exakt, was der Begriff verspricht: das Recht der Einzelnen, grundsätzlich selbst über die Erhebung, Speicherung, Verwendung und Weitergabe ihrer personenbezogenen Daten zu bestimmen.

Zwar wird weiter darauf hingewiesen, dass die Herleitung aus dem allgemeinen Persönlichkeitsrecht keineswegs zwingend sei, doch wird dieser Weg jedenfalls als gangbar anerkannt.[200] Da ein Kontrollverlust über die eigenen Daten zu den skizzierten Einschüchterungseffekten und zu Selbstzensur führen kann, kann er der Persönlichkeitsentwicklung schaden.[201] Vor diesem Hintergrund stellt sich die Verankerung des Rechts auf informationelle Selbstbestimmung im allgemeinen Persönlichkeitsrecht als sachgerecht dar, da sie den Gefahren für die Persönlichkeitsentwicklung Rechnung trägt.

Ergänzt wird das Recht auf informationelle Selbstbestimmung durch die jüngste Fortentwicklung des allgemeinen Persönlichkeitsrechts: das Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme, kurz: IT-Grundrecht. Es bewahrt über die Gewährleistungen durch das Recht auf informationelle Selbstbestimmung hinaus den persönlichen und privaten Lebensbereich der Grundrechtsträger vor staatlichem Zugriff im Bereich der Informationstechnik auch insoweit, als auf das informationstechnische System insgesamt zugegriffen wird und nicht nur auf einzelne Kommunikationsvorgänge oder gespeicherte Daten.[202] Geschützt ist das Interesse der Nutzer, dass die von einem informationstechnischen System erzeugten, verarbeiteten und gespeicherten Daten vertrau-

---

198 Eine aktuelle Aufarbeitung des Diskurses bietet: *Rupp*, Die grundrechtliche Schutzpflicht des Staates für das Recht auf informationelle Selbstbestimmung im Pressesektor, 2013, 64 ff.

199 *Starck*, in: Mangoldt/Klein (Hrsg.), Kommentar zum Grundgesetz Band I, 2010, Art. 2 Rn. 114.

200 *Britz*, Informationelle Selbstbestimmung zwischen rechtswissenschaftlicher Grundsatzkritik und Beharren des Bundesverfassungsgerichts, in: Hoffmann-Riem (Hrsg.), Offene Rechtswissenschaft, 2010, 561, 573 f. und *Hoffmann-Riem*, Informationelle Selbstbestimmung in der Informationsgesellschaft, in: ders. (Hrsg.), Offene Rechtswissenschaft, 2010, 499, 506.

201 Siehe oben Kapitel 3,A.II.2.

202 BVerfGE 120, 274 (313); zur verfassungsgerichtlichen Entwicklung des sogenannten IT-Grundrechts: *Hornung*, Grundrechtsinnovationen, 2015, 277 ff.

lich bleiben und dass die Integrität des geschützten informationstechnischen Systems nicht angetastet wird.[203] Schutz besteht somit allerdings hauptsächlich vor Gefahren, die nicht im direkten Zusammenhang mit informationeller Preisgabe stehen. Diese Konstellationen werden in der vorliegenden Arbeit nicht behandelt.[204]

In Zukunft zeichnet sich eine Ausweitung des Schutzes des allgemeinen Persönlichkeitsrechts um eine weitere Schutzdimension ab: um ein Recht auf Vergessenwerden. In diese Richtung geht *Diesterhöft*, wenn er überzeugend die Anerkennung eines „Rechts auf medialen Neubeginn" als Subdimension des allgemeinen Persönlichkeitsrechts fordert. Es würde den Bürgern die Befugnis verleihen, „grundsätzlich selbst über die Fortdauer der Abrufbarkeit identifizierender Informationen über das Internet bestimmen zu können".[205] Angesichts der aktuellen Diskussion erscheint es möglich, dass eine entsprechende Grundrechtsposition früher oder später Anerkennung finden wird.

b) *Europarechtliche Einflüsse*

Der Schutz informationeller Selbstbestimmung deutscher Bürger wird zunehmend auch durch die Schutzgewährleistungen der Europäischen Menschenrechtskonvention sowie der Europäischen Grundrechte-Charta erreicht.

Art. 8 EMRK schützt das Recht auf Achtung des Privatlebens. Der Schutzbereich ist weit und nicht abschließend definierbar. Jedenfalls umfasst er die körperliche und moralische Unversehrtheit und zahlreiche Aspekte der Identität der Einzelnen, etwa den Namen, das Recht am eigenen Bild und persönliche Informationen, von denen die Betroffenen berechtigterweise erwarten können, dass sie nicht ohne ihr Einverständnis veröffentlicht werden.[206] Der Europäische Gerichtshof für Menschenrechte hat in einer Vielzahl von Entscheidungen Gelegenheit zur Auslegung des Art. 8 EMRK gehabt. Hervorzuheben ist insbesondere seine sogenannte Caroline-Rechtsprechung, in der das Verhältnis zwischen dem Schutz des Privatlebens einerseits und dem Schutz der Meinungs- und Pressefreiheit andererseits ausgearbeitet wurde.[207]

Falls die Europäische Union der Europäischen Menschenrechtskonvention beitritt, wie es nach Art. 6 Abs. 2 EUV vorgesehen ist, entfaltet Art. 8 EMRK unmittelbare Rechtswirkung für die Europäische Union inklusive dem Europäischen Gerichtshof und für die Mitgliedstaaten, soweit sie Unionsrecht vollziehen.[208]

---

203 BVerfGE 120, 274 (314).

204 Siehe oben Kapitel 2,B.

205 *Diesterhöft*, Das Recht auf digitalen Neubeginn, 2014, 168.

206 St. Rspr., EuGH NJW 2014, 1645, 1646.

207 EGMR NJW 2004, 2647 ff. (Caroline I), NJW 2012, 1053 ff. (Caroline II) und NJW 2014, 1645 ff. (Caroline III); daran anknüpfend jüngst: EGMR NJW 2014, 3291 ff.; weiterführend: *Klass*, Der Schutz der Privatsphäre durch den EGMR im Rahmen von Medienberichterstattungen, ZUM 2014, 261 ff.

208 Zu den Auswirkungen eines Beitritts der Europäischen Union zur Europäischen Menschenrechtskonvention auf Deutschland: *Schaller*, Das Verhältnis von EMRK und deutscher Rechtsord-

Schon jetzt ist Art. 8 EMRK als allgemeiner Grundsatz des Unionsrechts über Art. 6 Abs. 3 EUV zu berücksichtigen, weil er Ausdruck der gemeinsamen Verfassungsüberlieferungen der Mitgliedstaaten ist.

In Deutschland steht die Europäische Menschenrechtskonvention lediglich im Rang einfachen Bundesrechts. Dennoch gilt der Grundsatz der EMRK-freundlichen Auslegung des Grundgesetzes, wie das Bundesverfassungsgericht in seiner Görgülü-Entscheidung darlegt.[209] Eine Verletzung dieses Grundsatzes kann als Verstoß gegen das jeweils einschlägige Grundrecht in Verbindung mit dem Rechtsstaatsprinzip durch Verfassungsbeschwerde gerügt werden. Zudem besteht nach Rechtswegerschöpfung (Art. 35 Abs. 1 EMRK) gemäß Art. 34 EMRK die Möglichkeit der Individualbeschwerde zum Europäischen Gerichtshof für Menschenrechte.

Auf europäischer Ebene gewährleisten zudem Art. 7 und 8 Abs. 1 GR-Ch und Art. 16 Abs. 1 AEUV (zuvor: Art. 286 Abs. 1 EG a. F.) den Schutz personenbezogener Daten. Art. 8 GR-Ch ist ein sogenanntes innovatives Grundrecht, seine Entstehungsgeschichte geht jedoch auf Art. 8 EMRK zurück.[210] Art. 7 und insbesondere 8 GR-Ch haben nach Art. 52 Abs. 3 GR-Ch die gleiche Bedeutung und Tragweite wie Art. 8 EMRK, soweit sie deckungsgleich sind. Ein weitergehender Schutz durch Art. 7 und 8 GR-Ch bleibt unberührt (Art. 52 Abs. 3 Satz 2 GR-Ch). Eine Entsprechung von Art. 8 EMRK und Art. 8 GR-Ch wird verneint; der Europäische Gerichtshof nimmt jedoch regelmäßig auf die Rechtsprechung zu Art. 8 EMRK Bezug.[211] Derzeit sei die Folgebereitschaft des Europäischen Gerichtshofs gegenüber dem Europäischen Gerichtshof für Menschenrechte sogar so hoch, dass es nach Einschätzung von *Britz* zu Abweichungen kaum kommen könne.[212]

Die Bejahung eines Eingriffs in Art. 7 und 8 GR-Ch hängt nicht davon ab, ob die erhobenen Daten sensibler Natur sind und ob die Betroffenen durch den Eingriff Nachteile erlitten haben können.[213] Die EU-Vorratsdatenspeicherungsrichtlinie griff beispielsweise in beide Grundrechte ein, da 1) Anbieter Daten auf Vorrat speichern mussten (Eingriff in Art. 7 GR-Ch), 2) nationale Behörden sich Zugang zu diesen Daten verschaffen konnten (ebenfalls Eingriff in Art. 7 GR-Ch) und 3) eine Verarbeitung personenbezogener Daten vorgesehen war (Eingriff in Art. 8

---

nung vor und nach dem Beitritt der EU zur EMRK, EuR 2006, 656. Das inzwischen ausgehandelte Beitrittsabkommen ist Ende 2014 im Gutachtenverfahren beim Europäischen Gerichtshof gescheitert, *Juris Redaktion*, EuGH-Gutachten: Entwurf der Übereinkunft über EU-Beitritt zur EMRK unionsrechtswidrig, 18.12.2014.

[209] BVerfGE 111, 307 (317 ff.).

[210] Erläuterung zu Art. 8 GR-Ch, ABl. 2007 C 303/21. Die Erläuterungen sind nach Art. 6 Abs. 1 UAbs. 3 EUV als Auslegungsanleitung zu berücksichtigen.

[211] *Britz*, Europäisierung des grundrechtlichen Datenschutzes?, EuGRZ 2009, 1, 2 f., 6 m. w. N. und *Streinz*, Die Rechtsprechung des EuGH zum Datenschutz, DuD 2011, 602, 604; umfassend zur Rechtsprechung der europäischen Gerichte: *Schiedermair*, Der Schutz des Privaten als internationales Grundrecht, 2012.

[212] *Britz*, Europäisierung des grundrechtlichen Datenschutzes?, EuGRZ 2009, 1, 3.

[213] EuGH EuZW 2014, 459 (461).

GR-Ch).[214] Das Ziel, den internationalen Terrorismus zum Schutz des Weltfriedens zu bekämpfen, stellte zwar einen legitimen Zweck dar.[215] Jedoch fehlte es angesichts der Bedeutung des Schutzes personenbezogener Daten und der Schwere und des Ausmaßes des Eingriffs an der Erforderlichkeit, da der Eingriff nicht auf das absolut Notwendige beschränkt war; Die Richtlinie war daher mit Art. 7 und 8 GR-Ch unvereinbar.[216]

Die Bedeutung der Art. 7 und 8 GR-Ch hat der Europäische Gerichtshof jüngst auch in der Entscheidung Google v. Costeja González weiter verdeutlich.[217] Dort entschied er, dass Art. 7 und 8 GR-Ch ein Recht gewähren, die Verlinkung auf bestimmte wahre Informationen in einer Suchmaschine verhindern zu lassen. Er führt aus, dass eine von einem Suchmaschinenbetreiber ausgeführte Verarbeitung personenbezogener Daten die Grundrechte auf Achtung des Privatlebens und Schutz personenbezogener Daten erheblich beeinträchtigen kann, wenn die Suche mit dieser Suchmaschine anhand des Namens einer natürlichen Person durchgeführt wird. Diese Verarbeitung ermöglicht es allen Internetnutzern, mit der Ergebnisliste einen strukturierten Überblick über die zu einzelnen Personen im Internet zu findenden Informationen zu erhalten, die potenziell zahlreiche Aspekte von deren Privatleben betreffen und ohne die betreffende Suchmaschine nicht oder nur sehr schwer hätten miteinander verknüpft werden können. Der Eingriff in die Rechte der Betroffenen wird noch gesteigert durch die bedeutende Rolle des Internets und der Suchmaschinen in der modernen Gesellschaft, die den in einer Ergebnisliste enthaltenen Informationen Ubiquität verliehen. Bei der Herstellung praktischer Konkordanz zwischen den Rechten der Suchmaschinenbetreiber und dem Informationsinteresse anderer Nutzer auf der einen Seite und den Rechten der Betroffenen auf der anderen Seite überwiegen im Allgemeinen die Interessen der Betroffenen. Zu berücksichtigen sind jedoch auch die Art der Informationen, die Sensibilität für das Privatleben der Betroffenen und das Informationsinteresse der Öffentlichkeit. Betroffene können nach der Entscheidung des Europäischen Gerichtshofs die Suchmaschinenbetreiber anweisen, aus der Liste mit den Ergebnissen einer anhand ihres Namens durchgeführten Suche Links zu von Dritten veröffentlichten Seiten mit Informationen über ihre Person zu entfernen.

---

[214] EuGH EuZW 2014, 459 (461).

[215] EuGH EuZW 2014, 459 (462).

[216] EuGH EuZW 2014, 459 (462 f.).

[217] Siehe zu den folgenden Ausführungen, soweit nicht anders angegeben: EuGH EuZW 2014, 541 (546 f.). Fragen der Zulässigkeit der Inhaltsangebote selbst waren nicht Thema der Entscheidung, sodass vorläufig offen bleibt, ob die Rechtsprechung des Bundesgerichtshofs, etwa in BGHZ 183, 353, Bestand haben wird, wonach Online-Archive unter den Bedingungen der Internetöffentlichkeit keine Pflicht haben, Altmeldungen aus dem Netz zu entfernen oder den Zugang zu erschweren; siehe auch: *Hornung/Hofmann*, Ein „Recht auf Vergessenwerden“?, JZ 2013, 163, 165 m. w. N.

In eine ähnliche Richtung geht auch Art. 17 EU-DS-GVO-E.[218] Dieser enthält jedenfalls dem Titel nach eine Regelung zur Einführung eines Rechts auf Vergessenwerden, umfasst jedoch de facto von einer erweiterten Nachberichtspflicht abgesehen kaum Neues. In der ursprünglichen Gestalt ist das Recht auf Vergessenwerden in der in erster Lesung durch das Europaparlament angenommenen Fassung der EU-Datenschutz-Grundverordnung nicht mehr enthalten.[219]

Art. 7 und 8 GR-Ch binden die Union sowie die Mitgliedstaaten bei der Durchführung des Rechts der Union (Art. 51 Abs. 1 Satz 1 GR-Ch), wobei strittig ist, wann von einer Durchführung des Unionsrechts auszugehen ist.[220] Der im Fall Åkerberg Fransson vom Europäischen Gerichtshof zugrunde gelegten weiten Auslegung[221] tritt das Bundesverfassungsgericht entschieden entgegen. Im Urteil zur Antiterrordatei stellt es fest, dass die genannte Entscheidung des Europäischen Gerichtshofs im Sinne eines kooperativen Miteinanders zwischen beiden Gerichten nicht in einer Weise interpretiert werden darf, in der die Entscheidung offensichtlich als Ultra-Vires-Akt zu beurteilen wäre oder den Schutz und die Durchsetzung der mitgliedstaatlichen Grundrechte in einer Weise gefährdete, dass dies die Identität der grundgesetzlichen Verfassungsordnung in Frage stelle. Insofern darf die Entscheidung nicht dahin gehend verstanden werden, dass für eine Bindung der Mitgliedstaaten durch die in der Grundrechte-Charta niedergelegten Grundrechte der Europäischen Union jeder sachliche Bezug einer Regelung zum bloß abstrakten Anwendungsbereich des Unionsrechts oder rein tatsächliche Auswirkungen auf dieses ausreichen.[222] Eine Durchführung des Unionsrechts liegt demnach nicht schon dann vor, wenn nationale Vorschriften Regelungsbereiche des Unionsrechts berühren oder das Funktionieren unionsrechtlich geordneter Rechtsbeziehungen mittelbar beeinflussen können.[223]

Kommt es jedoch tatsächlich zu einer Aufweichung des Art. 51 Abs. 1 Satz 1 GR-Ch, stellt sich die Frage nach den Auswirkungen auf den Privatheitsschutz in Deutschland, da sich dann mehr und mehr Sachverhalte aufgrund des Anwendungs-

---

[218] Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr (Datenschutz-Grundverordnung) v. 25.1.2012, KOM(2012) 11 endgültig, im Folgenden abgekürzt als: EU-DS-GVO-E.

[219] Im Folgenden abgekürzt als: LIBE-Fassung; Der derzeitige Stand ist abrufbar unter: http://www.janalbrecht.eu/fileadmin/material/Dokumente/DPR-Regulation-inofficial-consolidated-LIBE.pdf; zu den extrem komplexen – oder unmöglichen – technischen Voraussetzungen eines echten Rechts auf Vergessenwerden, siehe: *Hornung/Hofmann*, Ein „Recht auf Vergessenwerden“?, JZ 2013, 163, 168 f.

[220] Zum Streitstand: *Kingreen*, in: Calliess/Ruffert (Hrsg.), EUV, AEUV, 2011, Art. 51 GR-Ch, Rn. 7 ff.

[221] EuGH EuZW 2013, 302 (303 f.) (Åklagare v. Hans Åkerberg Fransson).

[222] BVerfGE 133, 277 (316); dazu: *Käß*, Das Urteil des Bundesverfassungsgerichts zum Antiterrordateigesetz, BayVBl 2013, 709 ff.

[223] BVerfGE 133, 277 (316).

vorrangs der Europäischen Grundrechtecharta nach dieser bestimmen würden.[224] Angesichts des faktischen Einflusses, den das deutsche Verfassungsrecht (in seiner Auslegung durch das Bundesverfassungsgericht) auf das Europarecht hat, ist jedoch, jedenfalls zunächst, wohl nicht von einschneidenden Änderungen in der deutschen Verfassungsordnung auszugehen.

c) *Anwendung auf den konkreten Fall*

Informationelle Preisgabe kann dazu führen, dass Nutzer angesichts eines Kontrollverlusts über ihre Daten Selbstzensur sowohl hinsichtlich der Quellenauswahl[225] als auch hinsichtlich des Erkenntnisprozesses üben.[226]

Durch das Recht auf informationelle Selbstbestimmung geschützte Interessen sind jedenfalls berührt, wenn die Nutzer tatsächlich Ziel von Überwachungsmaßnahmen etwa in der Form der Aufzeichnung und Auswertung aller Online-Tätigkeiten werden. Im Fall der informationellen Preisgabe steht jedoch häufig nicht fest, ob dies der Fall ist. Vielmehr kann die Selbstzensur bereits durch eine diffuse Angst vor solcher Überwachung ausgelöst werden, unabhängig davon, ob diese tatsächlich eintritt.[227] Es ist also zu klären, ob das Recht auf informationelle Selbstbestimmung auch vor Einschüchterungseffekten schützt, die das bloße Gefühl des Überwachtwerdens auslöst, unabhängig von der realen Faktenlage. Will das Recht auf informationelle Selbstbestimmung den Einzelnen das Recht geben, zu wissen, wer wann was über sie weiß, ist ein solcher „Schutz vor belastenden Gefühlen"[228] erfasst. Will es lediglich die Hoheit über die eigenen personenbezogenen Daten gewährleisten, fällt der Schutz vor befürchteter Überwachung aus dem Schutzbereich heraus.

In Richtung der letztgenannten Meinung könnte *Isensee* verstanden werden, wenn er ein „Grundrecht auf Freiheit vor Angst" ablehnt und davor warnt, dass es bei Anerkennung eines solchen Grundrechts dazu kommen könnte, dass der Staat als Reaktion auf „politisierte Ängste […] in Aktionismus verfällt und zur Abwehr von Putativgefahren und zur politischen Therapie von Angstpsychosen Grundrechtsbeschränkungen verfügt."[229] Er folgert jedoch einschränkend nur, dass der

[224] Zu den Folgen für Schutzpflichten aus Art. 7, 8 GR-Ch: *Streinz/Michl*, Die Drittwirkung des europäischen Datenschutzgrundrechts (Art. 8 GRCh) im deutschen Privatrecht, EuZW 2011, 384, 385 ff.

[225] Siehe oben Kapitel 3,A.II.2.b).

[226] Siehe oben Kapitel 3,A.II.2.c).

[227] Siehe oben Kapitel 3,A.II.2.

[228] *Bull*, Informationelle Selbstbestimmung, 2009, 61; vgl. *Oermann/Staben*, Mittelbare Grundrechtseingriffe durch Abschreckung, 52 Der Staat (2013), 630 ff.; kritisch: *Britz*, Informationelle Selbstbestimmung zwischen rechtswissenschaftlicher Grundsatzkritik und Beharren des Bundesverfassungsgerichts, in: Hoffmann-Riem (Hrsg.), Offene Rechtswissenschaft, 2010, 561, 574.

[229] *Isensee*, Das Grundrecht als Abwehrrecht und als staatliche Schutzpflicht, in: Isensee/Kirchhof (Hrsg.), Handbuch des Staatsrechts der Bundesrepublik Deutschland X, 2012, 413, 535, Rn. 255.

Staat nicht zur Verhinderung jedes Angstgefühls aufgerufen ist, sondern nur zu Bekämpfung der objektiven Gefahren, die begründete Furcht auslösen. Dieser Mittelweg erscheint sachgerecht.

Das Bundesverfassungsgericht betont in ständiger Rechtsprechung und hinsichtlich verschiedener Grundrechtspositionen den Zusammenhang zwischen der Furcht vor Überwachung und vorauseilender Selbstzensur.[230] Auf diesem Gedanken fußt schon die Argumentation im Volkszählungsurteil:[231] Die individuelle Selbstbestimmung setzt voraus, dass den Individuen „Entscheidungsfreiheit über vorzunehmende oder zu unterlassende Handlungen einschließlich der Möglichkeit gegeben ist, sich auch entsprechend dieser Entscheidung tatsächlich zu verhalten." Können sie nicht mit hinreichender Sicherheit überschauen, welche sie betreffenden Informationen in bestimmten Bereichen ihrer sozialen Umwelt bekannt sind und können sie das Wissen möglicher Kommunikationspartner nicht einigermaßen abschätzen, können sie in ihrer „Freiheit wesentlich gehemmt werden, aus eigener Selbstbestimmung zu planen oder zu entscheiden. […] Wer unsicher ist, ob abweichende Verhaltensweisen jederzeit notiert und als Information dauerhaft gespeichert, verwendet oder weitergegeben werden, wird versuchen, nicht durch solche Verhaltensweisen aufzufallen." Gerade um dieser Selbstbeschränkung der Handlungsweisen zu begegnen, bedurfte es der Entwicklung des Rechts auf informationelle Selbstbestimmung. Das Gericht hat den Grundrechtsschutz insoweit also vorverlagert.

Die im Volkszählungsurteil beschriebene Gefahr der Selbstzensur aus Angst vor Überwachung legte das Bundesverfassungsgericht in der Folge in zahlreichen Urteilen dar. So kann nach der ersten Entscheidung zur Telekommunikationsüberwachung die Befürchtung einer Überwachung schon im Vorfeld zu einer Befangenheit in der Kommunikation, zu Kommunikationsstörungen und zu Verhaltensanpassungen führen.[232] Die Entscheidung zum sogenannten Großen Lauschangriff stellt fest, dass von der Möglichkeit zur akustischen Wohnraumüberwachung Einschüchterungseffekte ausgehen können, da allein die Befürchtung einer Überwachung schon zu einer Befangenheit in der Kommunikation führen kann.[233] In den Entscheidungen zu den Anwaltsdaten und zu den Kommunikationsverbindungsdaten wird explizit ausgeführt, dass das Recht auf informationelle Selbstbestimmung über seinen unmittelbaren Gewährleistungsgehalt hinaus auch „vor einem Einschüchterungseffekt [schützt], der entstehen und zu Beeinträchtigungen bei der Ausübung anderer Grundrechte führen kann, wenn für den Einzelnen nicht mehr erkennbar ist, wer was wann und bei welcher Gelegenheit über ihn weiß."[234] In direkter Anlehnung an das Volkszählungsurteil gewährt die IMSI-Catcher-Entscheidung Schutz vor dem

---

[230] Siehe zu den zugrunde liegenden Überlegungen oben Kapitel 3,A.II.2.

[231] Siehe zu den folgenden Ausführungen, soweit nicht anders angegeben: BVerfGE 65, 1 (42 f.).

[232] BVerfGE 100, 313 (381).

[233] BVerfGE 109, 279 (354).

[234] BVerfGE 113, 29 (46) und 115, 166 (188).

Einschüchterungseffekt, der entstehen und zu Beeinträchtigungen bei der Ausübung anderer Grundrechte führen kann, wenn für die Einzelnen nicht mehr erkennbar ist, wann und innerhalb welcher Grenzen persönliche Sachverhalte offenbart sind. Die Freiheit der Einzelnen, aus eigener Selbstbestimmung zu planen und zu entscheiden, kann dadurch wesentlich gehemmt werden.[235] Weiter legt die Entscheidung zur Online-Durchsuchung dar, dass durch die vorgesehene Datenerhebung mittelbar die Freiheit der Bürger beeinträchtigt wird, „weil die Furcht vor Überwachung […] eine unbefangene Individualkommunikation verhindern kann."[236] Schließlich spricht die Entscheidung zur automatisierten Kennzeichenerfassung von allgemeinen Einschüchterungseffekten, die von der Ausübung von Grundrechten abhalten können und die individuellen Entfaltungschancen der Einzelnen beeinträchtigen. Dies ist insbesondere der Fall, wenn ein Gefühl des Überwachtwerdens entsteht.[237] Für das Fernmeldegeheimnis, das insoweit als sektorspezifische Ausprägung des Rechts auf informationelle Selbstbestimmung den identischen Rationalitäten unterliegt, formuliert das Bundesverfassungsgericht in der Entscheidung zur Vorratsdatenspeicherung von Telekommunikationsdaten schließlich, der Eingriff verfüge über eine „Streubreite, wie sie die Rechtsordnung bisher nicht kennt" und könne „ein diffus bedrohliches Gefühl des Beobachtetseins [… auslösen], das eine unbefangene Wahrnehmung der Grundrechte in vielen Bereichen beeinträchtigen kann".[238] Ohne dieses Urteil zu zitieren, aber in erkennbarer Aufnahme des Gedankens, spricht der Europäische Gerichtshof in seinem Urteil zur Vorratsdatenspeicherung davon, dass diese geeignet sei, bei den Bürgern „das Gefühl zu erzeugen, dass ihr Privatleben Gegenstand einer ständigen Überwachung ist."[239]

Den Auswirkungen, die schon die bloße Angst vor Beobachtung auf die Bürger haben kann, trägt schließlich der im Rahmen des Entwurfs des Beschäftigtendatenschutzgesetzes[240] vorgeschlagene § 32d Abs. 1 Satz 4 BDSG-E Rechnung, der Einrichtungen, die den Anschein einer Videoüberwachung hervorrufen, einer tatsächlichen Videoüberwachung gleichstellt.

Angesichts der schwerwiegenden Einschüchterungseffekte, die schon das Gefühl der Überwachtheit auslösen kann,[241] einerseits und der Unüberschaubarkeit von Informationszusammenhängen im Internet andererseits verlangt effektiver Grundrechtsschutz danach, jedenfalls Schutz vor dem Hervorrufen gravierender Einschüchterungseffekte zu gewähren. Führt informationelle Preisgabe dazu, dass

---

235 BVerfG NJW 2007, 351, 354.

236 BVerfGE 120, 274 (323).

237 BVerfGE 120, 378 (402, 430).

238 BVerfGE 125, 260 (318 ff.).

239 EuGH EuZW 2014. 459 (461).

240 Entwurf eines Gesetzes zur Regelung des Beschäftigtendatenschutzes, BT-Drs. 17/4230 v. 15.12.2010.

241 Siehe oben Kapitel 3,A.II.2. Eine aktuelle grundrechtliche Einordnung des „psychisch vermittelten Zwangs zur Selbstbeschränkung" bietet: *Diesterhöft*, Das Recht auf digitalen Neubeginn, 2014, 117 ff.

Nutzer aus der bloßen Angst vor negativen Folgen ihres Handelns Selbstzensur hinsichtlich der Quellenauswahl und des Erkenntnisprozesses üben, werden damit durch das Recht auf informationelle Selbstbestimmung geschützte Interessen berührt.

Es zeigt sich, dass die gefährdete informationelle Privatheit der Nutzer grundgesetzliche Absicherung durch das Recht auf informationelle Selbstbestimmung genießt. Bei der Auslegung dieses Rechts ist auch das Recht auf Achtung des Privatlebens (Art. 8 EMRK) zu berücksichtigen. Im Anwendungsbereich des Unionsrechts sind zudem Art. 7 und 8 GR-Ch einschlägig. Wie der Europäische Gerichtshof jüngst in der Entscheidung zur Vorratsdatenspeicherung ausführte, gilt dieser Schutz insbesondere, wenn eine Datenspeicherung und die spätere Nutzung der Daten erfolgen, ohne dass der Nutzer davon erfährt.[242]

2. Informationsfreiheit

Weiter könnten Interessen beeinträchtigt werden, die von der in Art. 5 Abs. 1 Satz 1 Halbsatz 2 GG verankerten Informationsfreiheit geschützt sind, da informationelle Preisgabe dazu führen kann, dass Nutzer zum einen an neutraler Quellenauswahl gehindert werden[243] und zum anderen aus Angst vor negativen Konsequenzen Selbstzensur hinsichtlich der Quellenauswahl üben.[244]

a) Funktion und Schutzbereich

Die Informationsfreiheit gewährleistet das Recht, sich ungehindert aus allgemein zugänglichen Quellen zu informieren. Nur ein umfassendes Informationsangebot, für das durch Zugang zu ausreichenden Informationsquellen Sorge getragen wird, ermöglicht eine freie Meinungsbildung.[245] Die Informationsfreiheit ist damit auch Voraussetzung der der Meinungsbildung folgenden Meinungsäußerung.

Eine Informationsquelle ist jeder Träger von Informationen.[246] Allgemein zugänglich ist eine Informationsquelle, wenn sie technisch geeignet und bestimmt ist, der Allgemeinheit, also einem individuell nicht bestimmbaren Personenkreis, Informationen zu verschaffen.[247] Das Internet ist eine solche allgemein zugängliche Informationsquelle.[248] Erfasst sind auch aus dem Ausland stammende Informationsquellen, solange die betreffenden Informationen in Deutschland empfangen werden können.[249]

---

242 EuGH EuZW 2014, 459 (461).
243 Siehe oben Kapitel 3,A.II.1.
244 Siehe oben Kapitel 3,A.II.2.b).
245 BVerfGE 27, 71 (81).
246 Beck-OK GG/*Schemmer*, 2015, Art. 5, Rn. 25.
247 BVerfGE 27, 71 (83).
248 Beck-OK GG/*Schemmer*, 2015, Art. 5, Rn. 26.
249 BVerfGE 90, 27 (32).

Geschützt sind das aktive Handeln zur Informationsverschaffung sowie die bloße Entgegennahme von Informationen.[250] Dabei wird auch die Entscheidung zur Information aus einer bestimmten Informationsquelle geschützt.[251] Ebenso vom Schutzbereich erfasst ist die negative Informationsfreiheit als das Recht, nicht informiert zu werden.[252] Letztere führt dazu, dass die Informationsfreiheit zum einen als Auswahlfreiheit verstanden werden muss und zum anderen Schutz vor fremdbestimmter Meinungsbildung gewährt.[253]

b) Europarechtliche Einflüsse

Auch die Informationsfreiheit ist europarechtlich gewährleistet. Art. 10 Abs. 1 Satz 2, 2. Alt. EMRK schützt das Recht, allgemein zugängliche Informationen und Ideen ohne behördliche Eingriffe und ohne Rücksicht auf Staatsgrenzen zu empfangen und weiterzugeben. Der Schutz ist nicht auf journalistische Quellen beschränkt,[254] sondern gilt auch gegenüber Privatpersonen.[255] Art. 10 EMRK schützt gerade auch die Kommunikation im Internet.[256]

Eine entsprechende Gewährleistung findet sich zudem in Art. 11 Abs. 1 Satz 2, 2. Alt. GR-Ch. Die in Satz 1 geschützte Meinungsfreiheit schließt dem Wortlaut des Art. 11 GR-Ch nach die Informationsfreiheit mit ein. Dadurch wird deutlich, dass der freie Zugang zu Informationen Grundlage für eine freie Meinungsäußerung ist. Vom Schutzbereich umfasst ist der gesamte Prozess des Sich-Informierens, also auch der Empfang, die Aufbereitung und die Speicherung von Informationen.[257]

Insbesondere eingeschlossen ist auch hier der Empfang von Informationen über das Internet. So bejahte der Europäische Gerichtshof beispielsweise einen Verstoß gegen die Informationsfreiheit im Falle einer Pflicht von Internetzugangsdiensten, eine sogenannte Peer-to-Peer-Filterung einzurichten, um Urheberrechtsverstöße zu verhindern.[258]

Hinsichtlich des Verhältnisses von Art. 10 Abs. 1 Satz 2, 2. Alt. EMRK und Art. 11 Abs. 1 Satz 2, 2. Alt. GR-Ch zueinander und den Auswirkungen auf die deutsche Rechtsordnung kann im Wesentlichen nach oben verwiesen werden.[259]

---

[250] BVerfGE 27, 1 (82).
[251] BVerfGE 90, 27 (38).
[252] Ausführlich dazu: *Fenchel*, Negative Informationsfreiheit, 1997.
[253] *Fenchel*, Negative Informationsfreiheit, 1997, 90.
[254] Dazu: EGMR NJW 2008, 2565 ff.; NJW-RR 2011, 1266 ff.; NJW 2013, 3709 ff.
[255] *Meyer-Ladewig*, in: ders. (Hrsg.), EMRK, 2011, Art. 10, Art. 10, Rn. 17.
[256] EGMR NJW 2013, 2735, 2736.
[257] Meyer-GRCh/*Bernsdorff*, 2014, Art. 11, Rn. 13.
[258] EuGH MMR 2012, 174, 176.
[259] Siehe oben Kapitel 3,B.I.1.b).

c) Anwendung auf den konkreten Fall

Durch informationelle Preisgabe können Nutzer an neutraler Quellenauswahl gehindert sowie von dem Zugang zu vermeintlich kontroversen Informationen abgehalten werden.

Da beide Umstände die Nutzer beim Zugang zu Informationen behindern können, werden Interessen berührt, die durch die in Art. 5 Abs. 1 Satz 1 Halbsatz 2 GG beziehungsweise Art. 10 Abs. 1 Satz 2, 2. Alt. EMRK und Art. 11 Abs. 1 Satz 2, 2. Alt. GR-Ch verankerte Informationsfreiheit geschützt sind.

II. Allgemeinwohlbelange

Weiter könnten durch informationelle Preisgabe verfassungsrechtlich geschützte Allgemeinwohlbelange beeinträchtigt werden, wenn die durch die informationelle Preisgabe gefährdete informationelle Privatheit Dritter (siehe 1.), der gesellschaftliche Fortschritt (siehe 2.) und die Demokratie (siehe 3.) verfassungsrechtlich geschützte Interessen darstellen.

1. Recht auf informationelle Selbstbestimmung Dritter

Neben zahlreichen anderen mittelbaren Gefahren kann informationelle Preisgabe insbesondere die informationelle Privatheit Dritter beeinträchtigen, wenn aus den preisgegebenen Daten Rückschlüsse auf diese Dritten gezogen werden können.[260] Dadurch müsste ein verfassungsrechtlich geschütztes Interesse tangiert sein.

Die informationelle Privatheit Dritter findet ebenso wie die informationelle Privatheit der Preisgebenden Schutz durch das Recht auf informationelle Selbstbestimmung.[261] Es gewährleistet den Dritten das Recht, selbst zu bestimmen, wann und innerhalb welcher Grenzen persönliche Sachverhalte offenbart werden.[262] Führt die Preisgabe dazu, dass Dritte betreffende Daten ohne deren Wissen oder gegen deren Willen veröffentlicht werden, verlieren sie die Möglichkeit, selbst über die Preisgabe und Verwendung ihrer Daten zu bestimmen. Dadurch werden durch das Recht auf informationelle Selbstbestimmung geschützte Interessen beeinträchtigt.[263]

2. Gesellschaftlicher Fortschritt

Weiter könnten durch die Preisgabe gesellschaftliche Belange von Verfassungsrang bedroht werden. Die möglicherweise entstehenden Gefahren fächern sich auf in die drei Teilaspekte kultureller, wissenschaftlicher und wirtschaftlicher Fortschritt.[264]

---

[260] Siehe oben Kapitel 3,A.III.1.

[261] Zu den dogmatischen Grundlagen: siehe oben Kapitel 3,B.I.1.

[262] BVerfGE 65, 1 (42).

[263] Zur Frage, ob der Staat die informationelle Selbstbestimmung Dritter schützen muss beziehungsweise darf: siehe unten Kapitel 5,A.VII und Kapitel 6,A.III.

[264] Siehe oben Kapitel 3,A.III.2.

Teilweise schlägt sich die Bedeutung dieser Belange in der Absicherung durch konkrete Grundrechte nieder. Darüber hinaus finden sie jedoch an zahlreichen anderen Stellen der Verfassung Erwähnung. Schon die Häufigkeit ihrer Nennung im Wortlaut des Grundgesetzes zeigt, dass diesen Belangen im gesellschaftlichen Gesamtsystem eine tragende Bedeutung zukommt.

Kultur[265] wird tangiert in Art. 5 Abs. 3 Satz 1, 1. Var. GG (Kunstfreiheit), Art. 29 Abs. 1 Satz 2, 2. Var. GG (kulturelle Zusammenhänge sind bei der Neugliederung des Bundesgebiets zu berücksichtigen), Art. 73 Abs. 1 Nr. 5a GG (ausschließliche Bundesgesetzgebungskompetenz über den Schutz deutschen Kulturgutes gegen Abwanderung ins Ausland).

Der Bereich der Wissenschaft findet Erwähnung in Art. 5 Abs. 3 Satz 1, 2. Var. GG (Wissenschaftsfreiheit), Art. 74 Abs. 1 Nr. 13, 2. Alt. GG (konkurrierende Gesetzgebungskompetenz zur Förderung der wissenschaftlichen Forschung), Art. 74 Abs. 1 Nr. 26 GG (konkurrierende Gesetzgebungskompetenz in der Genforschung) sowie Art. 91b GG (Zusammenwirken von Bund und Ländern im Bereich der Bildungsplanung und Forschungsförderung).

Aspekte der wirtschaftlichen Entwicklung sind in der Verfassung geregelt in Art. 12 GG (Berufsfreiheit), Art. 9 Abs. 3 Satz 1 GG (Koalitionsfreiheit), Art. 29 Abs. 1 Satz 2, 3. Var. GG (die wirtschaftliche Zweckmäßigkeit ist bei der Neugliederung des Bundesgebiets zu berücksichtigen), Art. 74 Abs. 1 Nr. 1 GG (Recht der Wirtschaft), Art. 91a Abs. 1 Nr. 1 GG (Mitwirkung des Bundes bei Länderaufgaben zur Verbesserung der regionalen Wirtschaftsstruktur) sowie Art. 104b Abs. 1 Satz 1 Nr. 3 GG (Finanzhilfen des Bundes an die Länder zur Förderung des wirtschaftlichen Wachstums).

Durch informationelle Preisgabe können tatsächliche Gefahren für den gesellschaftlichen Fortschritt in den drei genannten Bereichen entstehen. Dadurch werden Belange gefährdet, die entweder direkt grundrechtliche Absicherung genießen oder jedenfalls beiläufig mit Verfassungsrang ausgestattet sind.

3. Demokratie

Den überragenden Stellenwert, den das Grundgesetz der Demokratie zuweist, belegt zunächst ein Blick auf den Verfassungswortlaut. Das Grundgesetz bekennt sich zur Demokratie: Art. 20 Abs. 2 Satz 1 GG schreibt das Prinzip der Volkssouveränität vor, der anschließende Satz legt die Modi der Ausübung der Demokratie und damit Demokratie als Staats- und Regierungsform fest. Die in Art. 20 GG niedergelegten Grundsätze sind zudem von der Ewigkeitsgarantie des Art. 79 Abs. 3 GG geschützt.

[265] Eine ausführliche Analyse der Bedeutung kultureller Identität für den grundgesetzlichen freiheitlichen Verfassungsstaat bietet: *Uhle*, Freiheitlicher Verfassungsstaat und kulturelle Identität, 2004, 108 ff.

Informationelle Preisgabe kann nachteilige Auswirkungen auf das Gedeihen der Demokratie haben, da die Bürger die Möglichkeit zum Erkennen notwendiger Veränderungen verlieren oder gar nicht erst erlangen können, ihnen die notwendige Selbstbestimmtheit zur politischen Partizipation fehlen kann oder sie von politischer Teilnahme abgeschreckt werden können. Durch die einzelnen Gefahren müssten verfassungsrechtlich geschützte Interessen gefährdet werden.

Als Folge informationeller Preisgabe können Bürger davon abgehalten werden, die Informationen zu erhalten, die notwendig wären, um gesellschaftliche Veränderungen anzustoßen.[266] Vor den Gefahren, die eine eingeschränkte Informationsaufnahme für die Demokratie haben kann, schützt die Informationsfreiheit. Sie ist eine der wichtigsten Bedingungen der freiheitlichen Demokratie.[267] Durch sie werden Bürger in den Stand versetzt, sich selbst die notwendigen Voraussetzungen zur Ausübung ihrer persönlichen und politischen Aufgaben zu verschaffen, um im demokratischen Sinne verantwortlich handeln zu können. Mit zunehmender Informiertheit erkennen Bürger Wechselwirkungen in der Politik und deren Bedeutung und können schließlich daraus Folgerungen ziehen; ihre Freiheit zur Mitverantwortung und zur Kritik wächst. Nicht zuletzt können die Informationen die Einzelnen befähigen, die Meinungen Anderer kennenzulernen, sie gegeneinander abzuwägen, damit Vorurteile zu beseitigen und so Verständnis für Andersdenkende wecken.[268] Die Informationsfreiheit ist damit zudem Voraussetzung für die Ausübung der Meinungsfreiheit, die wiederrum essenziell für das Gedeihen der Demokratie ist.

Zudem können Bürger durch informationelle Preisgabe die intellektuelle Eigenständigkeit einbüßen, die notwendig wäre, um einen selbstbestimmten politischen Beitrag zu leisten.[269] Vor einer solchen Abschreckung schützt das Recht auf informationelle Selbstbestimmung. Das Bundesverfassungsgericht bringt im Volkszählungsurteil und in den Entscheidungen zum IMSI-Catcher und der automatisierten Kennzeichenerfassung den Zusammenhang zwischen der Funktionsfähigkeit der Demokratie und der Selbstbestimmtheit der Bürger zum Ausdruck, wenn es formuliert: „Individuelle Selbstbestimmung setzt […] voraus, daß dem Einzelnen Entscheidungsfreiheit über vorzunehmende oder zu unterlassende Handlungen […] gegeben ist“. Ihr Wegfall würde „das Gemeinwohl [beeinträchtigen], weil Selbstbestimmung eine elementare Funktionsbedingung eines auf Handlungsfähigkeit und

---

[266] Siehe oben Kapitel 3,A.III.3.a). Zum Einfluss von Suchmaschinen auf die demokratische Willensbildung: *Dörr/Natt*, Suchmaschinen und Meinungsvielfalt, ZUM 2014, 829, 830 ff. *Bunge* macht angesichts der durch Filter Bubbles entstehenden Gefahr für die öffentliche Meinungsbildung auch eine „kollektive Schutzrichtung“ des Rechts auf informationelle Selbstbestimmung aus, *Bunge*, Über die kollektive Schutzrichtung des Rechts auf informationelle Selbstbestimmung, 2015 ZD-Aktuell, 04635 ff.

[267] Generell zur Bedeutung der Kommunikationsgrundrechte für die Demokratie: *Starck*, Grundrechtliche und demokratische Freiheitsidee, in: Isensee/Kirchhof (Hrsg.), Handbuch des Staatsrechts der Bundesrepublik Deutschland III, 2005, 3 ff. Rn. 38 ff.

[268] BVerfGE 27, 71 (81 f.).

[269] Siehe oben Kapitel 3,A.III.3.b).

Mitwirkungsfähigkeit seiner Bürger begründeten freiheitlichen demokratischen Gemeinwesens ist."[270] Ein Verlust an individueller informationeller Selbstbestimmung zieht so unausweichlich einen Verlust an gesamtgesellschaftlicher demokratischer Substanz nach sich.[271] Wird durch informationelle Preisgabe die Selbstbestimmtheit der Bürger beeinträchtigt, wird damit das, durch das Recht auf informationelle Selbstbestimmung mittelbar geschützte, Interesse an der selbstbestimmten Teilnahme an demokratischen Prozessen tangiert.

Schließlich kann informationelle Preisgabe die Demokratie gefährden, indem Bürger von politischer Partizipation abgeschreckt werden können.[272] In gefestigter Rechtsprechung verbindet das Bundesverfassungsgericht das objektive Staatsziel, eine freiheitliche demokratische Grundordnung zu gewährleisten, mit dem Schutz des Rechts auf informationelle Selbstbestimmung. So führt es bereits im Volkszählungsurteil aus: „Wer damit rechnet, daß etwa die Teilnahme an einer Versammlung oder einer Bürgerinitiative behördlich registriert wird und daß ihm dadurch Risiken entstehen können, wird möglicherweise auf eine Ausübung seiner entsprechenden Grundrechte (Art. 8, 9 GG) verzichten."[273] Ebenso schränkt der durch heimliche Überwachung ausgelöste Einschüchterungseffekt die Kommunikation der Gesellschaft insgesamt ein.[274] Das Recht auf informationelle Selbstbestimmung in seiner Funktion als Hüter der Demokratie wird betroffen, wenn Nutzer infolge informationeller Preisgabe aus vorauseilendem Gehorsam von politischer Teilnahme absehen.

Einschüchterungseffekte können die Einzelnen zudem an der Ausübung von für die Demokratie essenziellen Rechten wie Meinungs- oder Versammlungsfreiheit hindern. Das Bundesverfassungsgericht anerkennt Meinungsfreiheit als schlechthin konstituierend für die freiheitlich-demokratische Staatsordnung, da sie die ständige geistige Auseinandersetzung, den Kampf der Meinungen, der das Lebenselement der Demokratie ist, ermöglicht.[275] Weiter stuft Gericht Versammlungsfreiheit als wesentliches Element demokratischer Offenheit ein, weil sich „im Kräfteparallelogramm der politischen Willensbildung im allgemeinen erst dann eine relativ richtige Resultante herausbilden kann, wenn alle Vektoren einigermaßen kräftig entwickelt sind."[276] Durch die Abschreckung von politischer Partizipation werden daher neben dem Recht auf informationelle Selbstbestimmung auch die Meinungs- und Versammlungsfreiheit berührt.

---

[270] In genannter Reihenfolge: BVerfGE 65, 1 (42 f.); BVerfG NJW 2007, 351, 354 und BVerfGE 120, 378 (430).

[271] *Simitis*, Die informationelle Selbstbestimmung, NJW 1984, 394, 399 f.

[272] Siehe oben Kapitel 3,A.III.3.c).

[273] BVerfGE 65, 1 (43).

[274] BVerfGE 100, 313 (381) und 109, 279 (354); vgl.: *Podlech*, Aufgaben und Problematiken des Datenschutzes, 5 DVR (1976), 23, 34 f.

[275] BVerfGE 7, 198 (208); siehe zum gerade im US-Recht präsenten Konzept des Marktplatzes der Ideen auch unten Kapitel 3,C.II.3.

[276] BVerfGE 69, 315 (346).

Zudem wird der Bedeutung der Demokratie an zahlreichen anderen Stellen innerhalb des Grundgesetzes Rechnung getragen: Art. 10 Abs. 2 Satz 2 GG (Beschränkungen des Brief-, Post- und Fernmeldegeheimnisses müssen den Betroffenen nicht mitgeteilt werden, wenn sie dem Schutz der freiheitlichen demokratischen Grundordnung dienen), Art. 11 Abs. 2 GG (Beschränkung der Freizügigkeit zum Schutz der freiheitlichen demokratischen Grundordnung), Art. 18 Satz 1 GG (Verwirkung von Grundrechten bei deren Missbrauch zum Kampf gegen die freiheitliche demokratische Grundordnung), Art. 21 Abs. 1 Satz 3 GG (die innere Ordnung von Parteien muss demokratischen Grundsätzen entsprechen), Art. 21 Abs. 2 Satz 1 GG (Verfassungswidrigkeit von Parteien, die bezwecken, die freiheitliche demokratische Grundordnung zu beeinträchtigen oder zu beseitigen), Art. 28 Abs. 1 Satz 1 GG (verfassungsmäßige Ordnung der Bundesländer muss demokratischen Grundsätzen entsprechen), Art. 73 Abs. 1 Nr. 10 lit. b GG (ausschließliche Bundesgesetzgebungskompetenz zum Schutz der freiheitlichen demokratischen Grundordnung), Art. 87a Abs. 4 Satz 1 GG (Einsatz der Streitkräfte zur Abwehr einer drohenden Gefahr für die freiheitliche demokratische Grundordnung) sowie Art. 91 Abs. 1 GG (Möglichkeit zur Anforderung von Polizeikräften anderer Länder sowie Kräften und Einrichtungen anderer Verwaltungen und des Bundesgrenzschutzes zur Abwehr von Gefahren für die freiheitliche demokratische Grundordnung).

Durch informationelle Preisgabe können Nutzer die Möglichkeit zum Erkennen notwendiger Veränderungen verlieren, die für politische Partizipation erforderliche Selbstbestimmtheit einbüßen oder von politischer Teilnahme abgeschreckt werden. Durch den Eintritt dieser Gefahren werden Interessen berührt, die Schutz durch die Informationsfreiheit, das Recht auf informationelle Selbstbestimmung, die Meinungsfreiheit, die Versammlungsfreiheit sowie zahlreiche andere grundgesetzliche Bestimmungen finden. Das Grundgesetz misst dem Schutz der Demokratie und der Bewahrung dieser Rechte gerade zum Schutz der Demokratie damit einen sehr hohen Stellenwert zu.

C. Gefährdete Rechtsgüter nach US-Verfassungsrecht

Zu klären ist, ob das US-Verfassungsrecht den durch informationelle Preisgabe bedrohten Interessen der Preisgebenden sowie der Allgemeinheit jeweils Verfassungsrang zumisst und wie gewichtig gegebenenfalls die jeweilige Stellung ist. Je bedeutender das Rechtsgut, desto eher kann sein Schutz als Eingriffsrechtfertigung für Maßnahmen zur Verhinderung informationeller Preisgabe dienen.[277]

Die US-Grundrechtsprüfung weicht im Aufbau erheblich von der deutschen ab: Während die Rechtfertigung von Eingriffen in die Grundrechte des Grundgesetzes typischerweise in den drei Stufen Schutzbereich, Eingriff, Rechtfertigung geprüft

[277] Siehe unten Kapitel 6,B.

wird, findet in den Vereinigten Staaten keine entsprechend strukturierte Prüfung statt. Vielmehr werden grundrechts- und kontextbezogene Analysen durchgeführt. Um der besseren Vergleichbarkeit willen wird im Rahmen dieser Arbeit eine dem deutschen Aufbau jedenfalls ähnliche Struktur gewählt, soweit dies angesichts des Wortlauts der Zusatzartikel und der Fallgruppenbildungen der Rechtsprechung sachgerecht erscheint.[278]

Das US-Verfassungsrecht ist nach einem Präzedenzfall-System (Case Law) ausgestaltet, in dem Gerichtsentscheidungen weit wichtiger sind als bei der Auslegung des Grundgesetzes. Über den bloßen Wortlaut des Verfassungstextes hinaus wird regelmäßig danach gefragt, welche Bedeutung (Original Meaning) der jeweiligen Vorschrift zum Zeitpunkt ihrer Abfassung zukam. Diese von *Justice Scalia* geprägte Auslegungsmethode stellt auf den Gehalt ab, den Durchschnittsmenschen dem Wortlaut zur damaligen Zeit beigemessen hätten, nicht jedoch auf verborgene Absichten der Verfassungsväter (Original Intent).[279] Anknüpfungspunkt für eine ausnahmsweise erweiternde Auslegung des Verfassungsrechts sind insbesondere die Due-Process-Klauseln des Fünften und 14. Zusatzartikels.[280]

Im Folgenden wird herausgearbeitet, welchen Stellenwert die US-Verfassung dem Schutz der bedrohten Rechtsgüter der Preisgebenden (siehe I) und der bedrohten Allgemeinwohlbelange zuschreibt (siehe II).

I. Rechtsgüter der Preisgebenden

Zunächst könnten die durch informationelle Preisgabe bestehenden Gefahren Rechtsgüter der Preisgebenden berühren. Die informationelle Privatheit findet keine explizite Absicherung gemäß den Zusatzartikeln, sodass ihr Schutz aus anderen Rechten abgeleitet werden muss.[281] Der U.S. Supreme Court hat hierzu bislang keine dem Volkszählungsurteil nahekommende wegweisende Entscheidung gefällt. In der Literatur scheint sich noch nicht einmal ein kleinster gemeinsamer Nenner ausmachen zu lassen, der in jedem denkbaren Privatheitszusammenhang vorläge. Dem trägt *Solove* Rechnung, wenn er feststellt: „privacy is not reducible to a singular essence; it is a plurality of different things that do not share one element in common

---

[278] *Brugger* weist zurecht daraufhin, dass eine Einteilung in Schutzbereich und Schranke im Wortlaut zahlreicher Zusatzartikel angelegt ist, auch wenn sie kaum Umsetzung in der Rechtsprechungspraxis findet: *Brugger*, Angloamerikanischer Einfluss auf die Grundrechtsentwicklung in Deutschland, in: Isensee/Kirchhof (Hrsg.), Handbuch des Staatsrechts der Bundesrepublik Deutschland X, 2012, 121 ff. Rn. 33.

[279] Vgl.: *Justice Scalia*, Constitutional Interpretation the Old Fashioned Way, 14.3.2005; *Balkin* versucht, den Gegensatz durch Etablierung eines „Living Originalism" zu überwinden, *Balkin*, Living originalism, 2011.

[280] *Lange*, Grundrechtsbindung des Gesetzgebers, 2010, 47 f.

[281] Die Rede ist daher von einem reduktionistischen Privatheitsverständnis, nach dem selbst in Situationen, die auf den ersten Blick Privatheitsbezug aufweisen, immer auch andere Güter tangiert sind: *Geuss*, Privatheit, 2002, 124 und *Thomson*, The Right to Privacy, 4 Philosophy & Public Affairs (1975), 295 ff.

but nevertheless bear a resemblance to each other."[282] Folglich schlägt er vor, Privatheit zu sehen als „a set of family resemblances".[283] Handeln, das Privatheit verletzten kann, teilt er in seiner „taxonomy of privacy" in vier Gruppen ein: Datensammlung, Datenverarbeitung, Datenverbreitung und Einbrüche in die Privatsphäre (die letzte Gruppe unterteilt er in körperliches Eindringen und die Einmischung in Entscheidungsfindungen).[284] Diese treffende Einteilung hilft hier jedoch nur begrenzt weiter, da ihr keine Aussagekraft über die verfassungsrechtliche Absicherung der einzelnen Privatheitsverletzungen zukommt. Im vorliegenden Kontext erscheint es daher sinnvoller, danach zu fragen, welche verfassungsrechtlichen Interessen durch die einzelnen Gefahren informationeller Preisgabe berührt werden:

Zunächst können Nutzer infolge informationeller Preisgabe Selbstzensur hinsichtlich der Quellenauswahl[285] und des Erkenntnisprozesses üben.[286] Vor dem zugrunde liegenden Kontrollverlust über die eigenen Daten könnten, ausgehend von dem Recht, alleine gelassen zu werden (siehe 1.), zum einen der Vierte Zusatzartikel (siehe 2.), zum anderen die Due-Process-Klauseln (siehe 3.) schützen.

Zudem könnte die gemäß dem Ersten Zusatzartikel geschützte Informationsfreiheit berührt sein, wenn durch informationelle Preisgabe die Quellenauswahl behindert wird[287] und die Nutzer Selbstzensur hinsichtlich der Quellenauswahl üben[288] (siehe 4.).

1. Recht, alleine gelassen zu werden

Aus dem Recht, alleine gelassen zu werden, könnten sich Erkenntnisse darüber ergeben, ob durch den Kontrollverlust über die eigenen Daten verfassungsrechtlich geschützte Interessen tangiert werden.

Ausgangspunkt des US-amerikanischen Privatheitsschutzes ist *Warrens* und *Brandeis'* Artikel „The Right to Privacy".[289] In diesem leiten sie ein Recht auf Privacy her, das sich aus einem Zusammenspiel der bestehenden rechtlichen Grundlagen zum Ehrschutz, Schutz von Geistigem Eigentum (insbesondere Urheberrecht),

---

[282] *Solove*, "I've Got Nothing to Hide" and Other Misunderstandings of Privacy, 44 San Diego L. Rev. (2007), 745, 756.

[283] *Solove*, Conceptualizing Privacy, 90 California L. Rev. (2002), 1087, 1126 ff.; *ders.*, "I've Got Nothing to Hide" and Other Misunderstandings of Privacy, 44 San Diego L. Rev. (2007), 745, 756 und *ders.*, Understanding Privacy, 2009, 39 ff.

[284] *Solove*, A Taxonomy of Privacy, 154 Univ. of Pennsylvania L. Rev. (2006), 477, 483 ff. und *ders.*, Understanding Privacy, 2009, 103 ff. Eine aktuelle Untersuchung dieses Konzepts liefert: *Wittmann*, Der Schutz der Privatsphäre vor staatlichen Überwachungsmaßnahmen durch die US-amerikanische Bundesverfassung, 2014, 464 ff.

[285] Siehe oben Kapitel 3,A.II.2.b).

[286] Siehe oben Kapitel 3,A.II.2.c).

[287] Siehe oben Kapitel 3,A.II.1.

[288] Siehe oben Kapitel 3,A.II.2.b).

[289] *Warren/Brandeis*, The Right to Privacy, 4 Harvard L. Rev. (1890), 193 ff.; deutsche Übersetzung: *Hansen/Weichert*, The Right to Privacy; ausführlich: *Solove/Schwartz*, Information Privacy Law, ³2009, 10 ff.

Eigentumsschutz, Verträgen beziehungsweise vertragsähnlichen Vertrauensverhältnissen und dem Schutz der Geschäftsgeheimnisse ergibt. Dieses Right to be let alone „secures to each individual the right to determining, ordinarily, to what extend his thoughts, sentiments, and emotions shall be communicated to others.“[290] *Warren* und *Brandeis* haben dabei den Schutz der Individuen vor privaten Akteuren, insbesondere der Presse, im Blick. Indem das Recht, alleine gelassen zu werden, soziale Grundsätze zum Zusammenleben der Bürger (Rules of Civility) bewahrt, schützt es so nicht nur die Individuen, sondern auch die Gesellschaft als solche.[291] Außer Acht bleibt zunächst das Verhältnis Bürger gegen Staat.

Später forderte *Justice Brandeis*, nunmehr in seiner Funktion als Richter am U.S. Supreme Court, durch das Recht, alleine gelassen zu werden, Privatheit im weiten Sinne zu schützen und es an die Schutzgewährleistungen der Zusatzartikel anknüpfen zu lassen: „Subtler and more far-reaching means of invading privacy have become available to the Government. Discovery and invention have made it possible for the Government, by means far more effective than stretching upon the rack, to obtain disclosure in court of what is whispered in the closet. [… T]he right to be let alone – the most comprehensive of rights, and the right most valued by civilized men.“[292]

Direkten verfassungsrechtlichen Niederschlag hat das Recht, alleine gelassen zu werden, jedoch nicht gefunden, sodass es ohne Erkenntnisse für die weitere Analyse bleibt.

2. *Vierter Zusatzartikel*

Weiter könnten die gemäß dem Vierten Zusatzartikel geschützten Rechte durch den Kontrollverlust über eigene Daten berührt sein, als dessen Folge Nutzer Selbstzensur hinsichtlich der Quellenauswahl und des Erkenntnisprozesses üben. Während in Deutschland das Recht auf informationelle Selbstbestimmung unproblematisch vor diesen Gefahren informationeller Preisgabe schützt, gestaltet sich die Situation in den USA schwieriger.

Die verfassungsrechtliche Absicherung der Privatheit in den Vereinigten Staaten wird maßgeblich geprägt durch Wortlaut und gerichtliche Auslegung des Vierten Zusatzartikels. Dieser lautet „The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no warrants shall issue, but upon probable cause, supported by oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.“ Der hierdurch gewährte Privatheitsschutz liegt begründet im Bedürfnis, Eigentum und Körper vor staatlichen Eingriffen zu schützen. Er ist anwendbar, wenn eine sogenannte Search oder Seizure vorliegt. Während eine Seizu-

[290] *Warren/Brandeis*, The Right to Privacy, 4 Harvard L. Rev. (1890), 193, 198.
[291] *Post*, The Social Foundations of Privacy, 77 California L. Rev. (1989), 957, 959 ff.
[292] Olmstead v. United States, 277 U.S. 438, 473 ff. (1928) (*Brandeis, J.*, dissenting).

re immer dann gegeben ist, wenn staatliche Akteure Kontrolle über Personen oder Sachen ausüben (in etwa vergleichbar mit einer Beschlagnahme nach deutschem Recht),[293] gestaltet sich die Beantwortung der Frage nach dem Vorliegen einer Search schwieriger. Diese findet im deutschen Recht kein direktes Äquivalent und lässt sich mit einer Durchsuchung, aber auch mit einer Telekommunikationsüberwachung vergleichen. Dem Wortlaut nach liegt sie im Fall von physischen Durchsuchungen vor, insbesondere durch staatliches Eindringen auf Grund und Boden der Rechtsträger. Eine Abkehr von diesem engen Verständnis lieferte die U.S.-Supreme-Court-Entscheidung Katz v. United States von 1967, nach der eine Search immer dann gegeben ist, wenn die berechtigte Privatheitserwartung (Reasonable Expectation of Privacy) der Rechtsträger durch aktives staatliches Handeln verletzt wird.[294] Dies ist der Fall, wenn eine subjektive Privatheitserwartung vorliegt, die die Gesellschaft als berechtigt anerkennt.[295]

Basis ist die subjektive, tatsächliche Erwartung der Privatheitsträger, ihre Privatheit werde gewahrt. Der Staat ist gehalten, diese Erwartung nicht durch die pauschale Ankündigung, jedwede Privatheit sei in Zukunft aufgehoben, zu zerstören. Läge ein solcher Fall vor, wäre das Kriterium der subjektiven Privatheitserwartung wohl normativ zu modifizieren, wie bereits in der U.S.-Supreme-Court-Entscheidung Smith v. Maryland angedeutet wird: „[I]f the Government were suddenly to announce […] that all homes henceforth would be subject to warrantless entry, individuals thereafter might not in fact entertain any actual expectation of privacy regarding their homes, papers, and effects. Similarly, if a refugee from a totalitarian country […] assumed that police were continuously monitoring his telephone conversations, a subjective expectation of privacy regarding the contents of his calls might be lacking as well. […] In determining whether a 'legitimate expectation of privacy' existed in such cases, a normative inquiry would be proper."[296]

Angesichts jüngster Enthüllungen[297] über Telekommunikationsüberwachungen der National Security Agency und insbesondere über das, durch den ehemaligen Geheimdienstmitarbeiter *Snowden* 2013 einer breiten Öffentlichkeit offengelegte, PRISM-Programm, wird man sich allerdings die Frage stellen müssen, inwieweit die subjektive Privatheitserwartung der Bürger tatsächlich noch reicht und ob die Zeit für eine normative Anpassung der Privatheitserwartung gekommen ist.

Des Weiteren muss die Gesellschaft bereit sein, diese subjektive Erwartung als reasonable anzuerkennen. Frei übersetzt muss die Angemessenheit oder Berechtigtheit der Erwartung festgestellt werden. Die Bewertung ist den Richtern überlassen,

---

[293] *Solove/Schwartz*, Privacy Law Fundamentals, 2013, 58.

[294] *Solove/Schwartz*, Privacy Law Fundamentals, 2013, 58.

[295] Katz v. United States, 389 U.S. 347, 361 (1967) (*Harlan, J.*, concurring).

[296] Smith v. Maryland, 442 U.S. 735, 741, Fn. 5 (1979).

[297] Eine juristische Analyse der Rechtmäßigkeit der in Rede stehenden geheimdienstlichen Überwachungstätigkeiten gestaltet sich schwierig, da es an offiziellen Informationen mangelt, sodass sich Untersuchungen weitestgehend auf Zeitungsberichte stützen müssen: *Ewer/Thienel*, Völker-, unions- und verfassungsrechtliche Aspekte des NSA-Datenskandals, NJW 2014, 30, 30 ff.

ohne Hinzuziehung einer Jury oder anderer Quellen (zu denken wäre beispielsweise an Befragungen der Bevölkerung oder Auswertung von Statistiken). Untersuchungen zeigen, dass Rechtsprechung und Empfinden der Testpersonen große Unterschiede darin aufweisen, ob an bestimmten Sachverhalten berechtigte Privatheitserwartungen bestehen. So ließ eine Studie Testpersonen auf einer Skala von 0 bis 100 einordnen, für wie einschneidend sie bestimmte Privatheitseingriffe befanden (100 als stärkster Eingriff). Die Untersuchung von Bankdaten, an denen nach United States v. Miller keine berechtigte Privatheitserwartung besteht, wurde beispielsweise mit 71,60 Punkten als starker Eingriff gewertet.[298] Jedenfalls aus dem Schutz ausgeschlossen sind jedoch solche Erwartungen, die lediglich ein Krimineller haben würde.[299]

Anhaltspunkte für die Beantwortung der Frage nach der Reasonableness der Privatheitserwartung bietet der Blick auf einschlägige Kasuistik:[300]

a) Schutz der Privatheit in der Öffentlichkeit

Grundlegend stellt sich die Frage, ob Vorgänge in der Öffentlichkeit qua definitionem dem Schutz des Vierten Zusatzartikels entzogen sind. Dies wäre der Fall, wenn nie begründete Privatheitserwartungen bestehen, sobald sich die Betroffenen in der Öffentlichkeit aufhalten.[301] Der schlichte Wortlaut des Vierten Zusatzartikels legt diese Annahme nahe, ist der Schutz doch stark mit dem eigenen Heim verknüpft. Dieser einschränkenden Auslegung ist jedoch der U.S. Supreme Court in Abkehr von früherer Rechtsprechung[302] in Katz v. United States entgegengetreten. Dort wurde ein belastendes Telefongespräch durch FBI-Beamte abgehört. Der Betroffene führte dieses Gespräch aus einer Telefonzelle heraus, auf deren Außenseite ein Abhörgerät angebracht war. Der Umstand, dass sich die Telefonzelle auf einer öffentlichen Straße befand, ist dem Schutz durch den Vierten Zusatzartikel nicht abträglich. Das Gericht führte aus: „For the Fourth Amendment protects people, not places. What a person knowingly exposes to the public, even in his own home or

---

[298] *Slobogin/Schumacher*, Reasonable Expectations of Privacy and Autonomy in Fourth Amendment Cases, 42 Duke L. J. (1993), 727, 738.

[299] Rakas v. Illinois, 439 U.S. 128, 150, Fn. 4 (1978).

[300] Eine aktuelle deutschsprachige Untersuchung der US-Rechtsprechung zur berechtigten Privatheitserwartung bietet auch: *Wittmann*, Der Schutz der Privatsphäre vor staatlichen Überwachungsmaßnahmen durch die US-amerikanische Bundesverfassung, 2014, 146 ff.

[301] Im Rahmen der Privatheitsforschung wird häufig unzutreffenderweise von einer „Großen Dichotomie“ ausgegangen und Privatheit schlicht als Gegenspielerin der Öffentlichkeit definiert. Schon im alten Griechenland wurde die Oikos, also die private Ordnung des Hauses, der Agora, dem Versammlungsplatz, gegenübergestellt. Auch ein Blick auf den lateinischen Wortursprung stützt diese Zweiteilung: Privare bedeutet soviel wie berauben, Privatus den sich nicht öffentlich betätigenden Bürger, der somit der öffentlichen Kontrolle entzogen ist. Markant ist der viel zitierte Ausspruch *Arendts*, der regelmäßig als Beleg für den Gegensatz Privatheit – Öffentlichkeit verstanden wird: „Der dunkle, verborgene Raum des Privaten bildete gleichsam die andere Seite des Öffentlichen“, *Arendt*, Vita Activa, [2]2003, 79.

[302] Olmstead v. United States, 277 U.S. 438 (1928).

office, is not a subject of Fourth Amendment protection. But what he seeks to preserve as private, even in an area accessible to the public, may be constitutionally protected."[303]

Auch besteht Privatheitsschutz in der Öffentlichkeit, wenn an Eingriffe in Eigentumsrechte angeknüpft werden kann. So schützt der Vierte Zusatzartikel vor GPS-Überwachung durch die Polizei, wenn diese ein GPS-Gerät am Auto der Betroffenen anbringt und damit eine Überschreitung hinsichtlich des Eigentums stattfindet. Dieser Begründungsansatz ist jedoch nicht unumstritten, als Lösung wird eine Interpretation des Vierten Zusatzartikels unabhängig vom Eigentumsinteresse gefordert, die sich an der Schwere des Eindringens in die Privatheit orientiert. So bemängelt eine der Concurring Opinions in United States v. Jones: „Court's reasoning largely disregards what is really important (the use of a GPS for the purpose of long-term tracking) and instead attaches great significance to something that most would view as relatively minor (attaching to the bottom of a car a small, light object that does not interfere in any way with the car's operation)."[304]

b) *Misplaced-Trust-Doktrin*

Vertrauen ist wichtig, doch trägt jeder selbst die Verantwortung, seine Vertrauten sorgfältig auszuwählen. Diese Erkenntnis lässt sich aus der Misplaced-Trust-Doktrin ziehen. Demnach entfällt der Schutz, wenn die Betroffenen Anderen Geheimnisse anvertrauen und diese das in sie gesetzte Vertrauen missbrauchen. So geschah es in Hoffa v. United States, als Geheimnisse einem Undercover-Agenten und vermeintlichen Freund offenbart wurden.[305] Entsprechendes galt in Lewis v. United States, als sich ein Undercover-Agent als vermeintlicher Drogenankäufer ausgab.[306] Die Bewertung ändert sich auch nicht, wenn Undercover-Agenten die belastenden Gespräche mit einem Aufnahmegerät mitzeichnen[307] oder ein Gerät bei sich tragen, welches die Gespräche simultan an ein anderenorts gelegenes Aufnahmegerät oder andere Agenten überträgt.[308] Auch die Kombination von Misplaced-Trust-Doktrin und dem Einsatz technischer Aufnahmemöglichkeiten ist keineswegs unumstritten. Bezeichnend sind die Dissenting Opinions in United States v. White: *Justice Douglas* führt aus: „What the ancients knew as ‛eavesdropping' we now call ‛electronic surveillance,' but to equate the two is to treat man's first gunpowder on the same level as the nuclear bomb. [… M]ust everyone live in fear that every word he speaks may be transmitted or recorded and later repeated to the entire world? I can imagine nothing that has a more chilling effect on people speaking their minds and

---

303 Katz v. United States, 389 U.S. 347, 351 (1967).

304 United States v. Jones, 132 S.Ct. 945, 961 (2012) (*Alito*, *Ginsburg*, *Breyer*, *Kagan*, *JJ.*, concurring).

305 Hoffa v. United States, 385 U.S. 293 (1966).

306 Lewis v. United States, 385 U.S. 206 (1966).

307 Lopez v. United States, 373 U.S. 427 (1963).

308 On Lee v. United States, 343 U.S. 747 (1952).

expressing their views on important matters. The advocates of that regime should spend some time in totalitarian countries and learn first-hand the kind of regime they are creating here."[309] Ginge es nach *Justice Douglas*, müsste die Misplaced-Trust-Doktrin demnach angesichts moderner Überwachungsmöglichkeiten erheblich gelockert werden, um den Bürgern noch angemessenen Schutz durch den Vierten Zusatzartikel bieten zu können. Auch *Justice Harlan* zeigt sich kritisch: „Were third-party bugging a prevalent practice, it might well smother that spontaneity – reflected in frivolous, impetuous, sacrilegious, and defiant discourse that liberates daily life. Much off-hand exchange is easily forgotten, and one may count on the obscurity of his remarks, protected by the very fact of a limited audience, and the likelihood that the listener will either overlook or forget what is said, as well as the listener's inability to reformulate a conversation without having to contend with a documented record."[310] Beide befürchten also, dass die Furcht vor allgegenwärtiger staatlicher Beobachtung Gefahren für die intellektuelle Privatheit hervorbringt, die den durch informationelle Preisgabe ausgelösten vergleichbar sind.[311]

Den kritischen Stimmen ist beizupflichten. Gesellschaftliche Kommunikation bedarf des Vertrauens darein, dass sich die Gegenüber an gebräuchliche Normen halten. Daher darf jedenfalls nicht jedes in Dritte gesetzte Vertrauen als unberechtigt gewertet werden, da sonst die Gesellschaft insgesamt leidet.

c) Plain-View-Doktrin

Sobald etwas offen sichtbar ist, besteht keine berechtigte Privatheitserwartung mehr.[312] Diese Erkenntnis erscheint zunächst nicht weiter überraschend. Und doch gibt es Fälle, in denen die Betroffenen sehr wohl jedenfalls subjektiv von der Achtung ihrer Privatheit ausgehen. Zu denken ist beispielsweise an den Sachverhalt, der der Entscheidung Florida v. Riley zugrunde liegt. Dort verschafften sich Ermittlungsbeamte Kenntnis über das Innere eines Gewächshauses, indem sie mit einem Helikopter in niedriger Höhe darüberflogen und durch Lücken im Dach spähten.[313] Nach Ansicht des Gerichts besteht hier keine berechtigte Privatheitserwartung. Dieses Ergebnis wird jedoch zurecht von einer der Dissenting Opinions abgelehnt unter Hinweis darauf, dass *Orwell* ein solches Vorgehen explizit als Teil seiner Horrorvision in „Nineteen Eighty-Four" skizziert.[314]

Ebenfalls besteht kein Schutz bei von einem Flugzeug aus geschossenen Luftbildern, die von einem penibel zur Seite und gegen tieffliegende Luftfahrzeuge geschützten Gelände aufgenommen wurden.[315]

---

309 United States v. White, 401 U.S. 745, 756 ff. (1971) (*Douglas, J.*, dissenting).
310 United States v. White, 401 U.S. 745, 787 ff. (1971) (*Harlan, J.*, dissenting).
311 Siehe oben Kapitel 3,A.II.2.
312 Harris v. United States, 390 U.S. 234 (1968).
313 Florida v. Riley, 488 U.S. 445 (1989).
314 Florida v. Riley, 488 U.S. 445, 466 (*Brennan*, *Marshall, Stevens*, *JJ*., dissenting).
315 Dow Chemical Co. v. United States, 476 U.S. 227 (1986).

Auch diese Doktrin bedarf einer kritischen Würdigung. Wie der Hinweis auf „Nineteen Eighty-Four“ zeigt, führt eine konsequente Anwendung der Plain-View-Doktrin zu Situationen, die eher den Angstvorstellungen der Bevölkerung gleichen als einer wünschenswerten Umsetzung des Verfassungsrechts. Die öffentliche Sichtbarkeit (Plain View) eines Gegenstands ist daher dann abzulehnen, wenn er nur unter großen Anstrengungen und eben nicht von jedermann wahrgenommen werden kann.

d) *Third-Party-Doktrin*

Eine berechtigte Privatheitserwartung wird ausgeschlossen, sobald die Betroffenen ihre Informationen Dritten zugänglich machen. So besteht die Erwartung nicht hinsichtlich Bankdaten, die der Bankkunde seiner Bank mitteilte und die diese an die Ermittlungsbehörden gab.[316] Gleiches gilt im Falle des Mitzeichnens der gewählten Telefonnummern durch Ermittlungsbehörden. Da der Telefonkunde weiß, dass jedenfalls seinem Telefonanbieter die gewählten Telefonnummern bekannt sind, besteht keine berechtigte Privatheitserwartung hinsichtlich der Nummern. Der U.S. Supreme Court führt aus: „[W]e doubt that people in general entertain any actual expectation of privacy in the numbers they dial. All telephone users realize that they must ‘convey’ phone numbers to the telephone company, since it is through telephone company switching equipment that their calls are completed.“[317]

Bislang fehlt es an einer höchstrichterlichen Aufarbeitung der Frage, ob und in welchem Umfang die Third-Party-Doktrin auch im Internetkontext und insbesondere bei der Überwachung von E-Mails anzuwenden ist. Die Instanzgerichte bejahen die Frage weitgehend, im Einzelnen bestehen jedoch Unklarheiten:

Verbindungsdaten stellen keine geschützten Inhaltsdaten (Content) dar, sondern unterfallen regulär der Third-Party-Doktrin, sodass sie de facto ungeschützt sind.[318] Aus dem Schutz heraus fallen sogar Metadaten, die im Zusammenhang mit einem via Smartphone aufgenommenen Foto gespeichert wurden, ohne dass die Existenz solcher Metadaten den Betroffenen bewusst war.[319]

Entsprechend handelt es sich auch bei E-Mail-Headers, IP-Adressen und der Information über die genutzten Datenmengen nicht um Inhaltsdaten.[320] Ebenfalls be-

---

316 United States v. Miller, 425 U.S. 435 (1976).

317 Smith v. Maryland, 442 U.S. 735, 742 (1979).

318 Smith v. Maryland, 442 U.S. 735, 741 (1979).

319 United States v. Post, 997 F.Supp.2d 602, 605 f. (S.D. Tex. 2014).

320 „[E]-mail and Internet users have no expectation of privacy in the to/from addresses of their messages or the IP addresses of the websites they visit because they should know that this information is provided to and used by Internet service providers for the specific purpose of directing the routing of information. […] Second, e-mail to/from addresses and IP addresses constitute addressing information and do not necessarily reveal any more about the underlying contents of communication than do phone numbers.“, United States v. Forrester, 512 F.3d 500, 503 (9th Cir. 2007). Anders werten Grundgesetz und Europäische Menschenrechtskonvention, welche diesen den Schutz des Telekommunikationsgeheimnisses gewähren.

steht keine berechtigte Privatheitserwartung an Benutzerdaten, die Internet-Service-Providern zur Verfügung gestellt werden.[321] Jüngst hat der District Court im südlichen Distrikt New York für Aufsehen gesorgt, als er de facto einen Schutz privater E-Mails durch den Vierten Zusatzartikel mit der Begründung ablehnte: „When we use a computer network such as Internet, however, a user does not have a physical 'home,' nor really any private space at all."[322] Diese Entscheidung ist aus internationaler Sicht umso besorgniserregender, als das Gericht zudem die ermittlungsbehördliche Beschlagnahme von E-Mails, die auf ausländischen Servern gespeichert sind, für zulässig erklärt. Solange die E-Mails erst in den USA von Ermittlungsbehörden ausgewertet werden, liegt keine Extraterritorialität vor.[323] Da ohne eine solch weite Auslegung die Tätigkeiten der Ermittlungsbehörden stark erschwert wären, ist es unwahrscheinlich, dass der Kongress eine enge Auslegung bei Erlass der zugrunde liegenden Normen beabsichtigt hat.[324] Die erforderliche Auseinandersetzung mit dem völkerrechtlichen Souveränitätsgrundsatz findet jedoch nicht statt. Angesichts starker Proteste aus Wissenschaft und Praxis bleibt abzuwarten, ob diese bedenkliche, nicht rechtskräftige Entscheidung aufrechterhalten bleibt.[325]

Die Third-Party-Doktrin ist nicht unumstritten und steht insbesondere dem europäischen Prinzip der Zweckbindung diametral entgegen.[326] Angesichts der Allgegenwärtigkeit technologischer Entwicklungen müssen Bürger annehmen, dass beinahe alle sie betreffenden Daten irgendjemandem bekannt sind. Dennoch scheint es nicht ausgeschlossen, dass die Mehrheit davon ausgeht, personenbezogene Daten nur in bestimmten Verwendungszusammenhängen preiszugeben. *Nissenbaum* appelliert entsprechend, Privatheit kontextbezogen zu betrachten und die vom Grundrechtsträger gesetzten Kontexte zu achten. Bei ehrlicher Betrachtung dürfte niemand mehr über eine berechtigte Privatheitserwartung verfügen. Daher biete sich ein neues Konzept der kontextuellen Integrität an. Diese sei verletzt, wenn preisgegebene Daten entweder unangebracht verwendet oder entgegen der Absprache verbreitet werden.[327] Während die Idee der kontextuellen Integrität aus deutscher Sicht nur eine Selbstverständlichkeit auszudrücken scheint, ist sie ein begrüßenswerter Ansatzpunkt, um ein Ausufern der US-amerikanischen Third-Party-Doktrin zu erreichen.

---

321 *United States v. Hambrick,* 55 F. Supp.2d 504 (4th Cir. 1999).

322 Microsoft v. United States, 15 F.Supp.3d 466, 471 (S.D.N.Y. 2014); zum Verfahren: *Mullin*, Microsoft agrees to contempt order so e-mail privacy case can be appealed, 10.9.2014; *Spies*, Berufungsverfahren Microsoft v. USA, ZD-Aktuell 2015, 04558 ff.

323 Microsoft v. United States, 15 F.Supp.3d 466, 472 (S.D.N.Y. 2014).

324 Microsoft v. United States, 15 F.Supp.3d 466, 474 (S.D.N.Y. 2014).

325 Derzeit ist das Rechtsmittelverfahren vor dem Second Circuit Court anhängig.

326 So auch: *Weichert*, Privatheit und Datenschutz im Konflikt zwischen den USA und Europa, RDV 2012, 113, 115.

327 *Nissenbaum*, Privacy as Contextual Integrity, 79 Washington L. Rev. (2004), 119, 136 ff.; *dies.*, Privacy in context, 2010 und *dies.*, A Contextual Approach to Privacy Online, Daedalus, the Journal of the American Academy of Arts & Sciences 2011, 32 ff. Eine aktuelle Analyse von *Nissenbaums* Ansatz liefert: *Wittmann*, Der Schutz der Privatsphäre vor staatlichen Überwachungsmaßnahmen durch die US-amerikanische Bundesverfassung, 2014, 489 ff.

Auch lässt sich fragen, ob die Third-Party-Doktrin zur Anwendung kommen darf, wenn den Rechtsträgern keine (echte) Möglichkeit offensteht, die Einbeziehung von Dritten zu umgehen. Schon die Dissenting Opinion in Smith v. Maryland zeigt sich kritisch: „[U]nless a person is prepared to forgo use of what for many has become a personal or professional necessity, he cannot help but accept the risk of surveillance. It is idle to speak of 'assuming' risks in contexts where, as a practical matter, individuals have no realistic alternative. […] In my view, whether privacy expectations are legitimate within the meaning of Katz depends not on the risks an individual can be presumed to accept when imparting information to third parties, but on the risks he should be forced to assume in a free and open society."[328] Jedenfalls wenn die Preisgebenden nicht in zumutbarer Weise auf die Einschaltung von Dritten verzichten konnten, scheint es angebracht, ihnen nicht die vollen Risiken deren Einbeziehung aufzuerlegen und somit die Third-Party-Doktrin nicht zur Anwendung kommen zu lassen. Folgt man diesem Einschränkungsvorschlag, wird der Anwendungsbereich der Third-Party-Doktrin im Internetkontext erheblich verringert.

Angesichts der uneinheitlichen Rechtslage hinsichtlich des Schutzes von E-Mails, die (auch) auf den Servern von Internet-Service-Providern (also Dritten) gespeichert sind,[329] haben große Konzerne wie Google,[330] Facebook[331] und Yahoo[332] einseitig angekündigt, nur gegen Vorlage von Warrants (im deutschen Recht vergleichbar mit Durchsuchungsbefehlen) Inhaltsdaten von E-Mails et cetera gegenüber Ermittlungsbehörden offenzulegen.

Um der Gefahr einer vollständigen Erosion des Schutzes durch den Vierten Zusatzartikel zu begegnen, erscheint eine Aufweichung der Third-Party-Doktrin wahrscheinlich. Andernfalls lässt sich ein Szenario malen, in dem nur noch privat ist, was in Isolation und insbesondere ohne Zuhilfenahme von Internettechnologien erfolgt. Entsprechend wird geraten: „go live as a hermit in a cabin on a mountaintop. That's where the Fourth Amendment still protects you."[333] Bis dato findet sich diese Aufweichung jedoch noch nicht in der Rechtsprechung wieder.

e) Die Sinne verstärkende Technologien

Angesichts kontinuierlichen technischen Fortschritts stellt sich die Frage, inwieweit eine berechtigte Privatheitserwartung an Umständen besteht, die nur dank die Sin-

---

[328] Smith v. Maryland, 442 U.S. 735, 750 (1979) (*Marshall*, *Brennan*, *JJ.*, dissenting).

[329] United States v. Warshak, 631 F.3d 266 (6th Cir. 2010): Warrant für E-Mails immer erforderlich; Theofel v. Farey Jones, 359 F.3d 1066 (9th Cir. 2004): Warrant erforderlich für E-Mails, die maximal 180 Tage beim Internet-Service-Provider gespeichert sind.

[330] http://www.google.com/transparencyreport/userdatarequests/legalprocess/#what_does_google_do.

[331] https://www.facebook.com/safety/groups/law/guidelines/.

[332] http://www.wired.com/threatlevel/2013/01/yahoo-demands-warrants/.

[333] *Solove*, Nothing to Hide, 2011, 110.

ne verstärkender Technologien erkennbar werden, nicht jedoch mit bloßem Auge, Ohr, Geruchssinn et cetera. Schon am Einsatz von Spürhunden scheiden sich die Geister.[334] Generell soll danach unterschieden werden, welche Verbreitung die in Rede stehende Technologie im Alltagsleben gefunden hat. Nur, wenn sie nicht im generellen öffentlichen Gebrauch ist, besteht eine berechtigte Privatheitserwartung. Eine solche Erwartung ist nach der U.S.-Supreme-Court-Entscheidung Kyllo v. United States zu bejahen, wenn Ermittlungsbehörden die Außenseite eines Hauses mit einem Wärmemesser absuchen, um (mit Hitze verbundenen) Marihuana-Anbau im Haus zu entdecken.[335] Fernliegend scheint hingegen die Dissenting Opinion: „this case involves nothing more than off-the-wall surveillance by law enforcement officers to gather information exposed to the general public from the outside of petitioner's home. […] Heat waves, like aromas that are generated in a kitchen, or in a laboratory or opium den, enter the public domain if and when they leave a building. A subjective expectation that they would remain private is not only implausible but also surely not one that society is prepared to recognize as 'reasonable.'"[336] Würde sich die letztgenannte Meinung durchsetzen, müssten Menschen nicht nur außerhalb, sondern auch innerhalb ihres Hauses ihr tatsächliches Verhalten jederzeit so gestalten, als ob sie Ziel staatlicher Überwachung sein könnten. Dies würde zu gravierender Selbstzensur führen und auf Dauer die Persönlichkeit der Menschen verarmen lassen.[337]

f) Anwendung auf den konkreten Fall

Informationelle Preisgabe kann dazu führen, dass Nutzer nicht mehr wissen können, wann und innerhalb welcher Grenzen persönliche Sachverhalte offenbart sind. In der Folge kann es zu Selbstzensur hinsichtlich der Quellenauswahl und des Erkenntnisprozesses kommen.

Es erscheint jedoch zweifelhaft, ob durch diesen Kontrollverlust Interessen berührt werden, die nach Maßgabe der bisherigen Rechtsprechung vom Vierten Zusatzartikel erfasst sind. Dieser schützt vor staatlichen Maßnahmen, die in die informationelle Privatheit der Nutzer eingreifen, wenn diese eine berechtigte Privatheitserwartung haben. Eingeschlossen ist an sich auch jede Form von informationeller Preisgabe im Internet, selbst wenn man deren Schutz als Privatheitsschutz in der Öffentlichkeit werten würde.[338]

---

[334] United States v. Place, 462 U.S. 696 (1983); Illinois v. Caballes, 543 U.S. 405 (2005); Florida v. Harris, 133 S.Ct. 1050 (U.S. 2013) und Florida v. Jardines, 133 S.Ct. 1409 (U.S. 2013).

[335] Kyllo v. United States, 533 U.S. 27 (2001).

[336] Kyllo v. United States, 533 U.S. 27, 42 (2001) (*Stevens, J., Rehnquist, C.J., O'Connor, Kennedy, JJ.*, dissenting).

[337] Zur Auswirkung von Überwachung auf menschliches Verhalten siehe oben Kapitel 3,A. II.2.a).

[338] Siehe oben Kapitel 3,C.I.2.a).

Jedoch wird davon auszugehen sein, dass der Schutz nach der Misplaced-Trust-Doktrin[339] entfällt, wenn Nutzer ihre Daten ihrem Online-Anbieter anvertrauen und dieser das Vertrauen missbraucht, beispielsweise durch mehr oder weniger freiwillige Weitergabe der Daten an staatliche Stellen.

Ebenso kann der Schutz nach einer entsprechenden Anwendung der Plain-View-Doktrin[340] entfallen, wenn im Internet preisgegebene Daten für Ermittlungsbehörden aufgrund technischer oder menschlicher Fehler einsehbar sind, selbst wenn dies den Preisgebenden nicht bewusst sein muss.

Jedenfalls soll staatlicher Zugriff mangels berechtigter Privatheitserwartung zulässig sein, wenn die Daten einem Dritten gegenüber preisgegeben werden (Third-Party-Doktrin).[341] Die Rechtslage ist unklar, doch wird man nach derzeitigem Stand wohl davon ausgehen müssen, dass der Schutz von Internetaktivitäten durch den Vierten Zusatzartikel vernachlässigbar gering ausfällt, da die Daten schon aus technischer Notwendigkeit durch die Hände (oder Computer) Dritter fließen und damit keine berechtigte Privatheitserwartung besteht.

Es kommt damit regelmäßig schon nicht mehr darauf an, dass Nutzer auch den Einsatz von Überwachungstechnologien oder Datenanalysetools, die die Sinne verstärken, befürchten müssen, welche bereits im Alltagsleben verbreitet sind.[342] Haben die Nutzer von der Anwendung dieser Technologien auszugehen, würde auch aus diesem Grund der Schutz des Vierten Zusatzartikels entfallen.

Wenn der Vierte Zusatzartikel jedoch schon keinen Schutz vor staatlicherseits erzeugten Gefahren informationeller Preisgabe bietet, lässt sich aus ihm erst recht kein Argument dafür gewinnen, dass der Verfassung an dem Schutz der informationellen Privatheit vor durch Private erzeugte Gefahren gelegen wäre. Der Vierte Zusatzartikel kann daher nach jetzigem Stand seiner Auslegung nicht als Maßstab für die weitere Analyse herangezogen werden.

3. Due-Process-Klauseln

Weiter könnten durch den Kontrollverlust über Daten, der zur Selbstzensur hinsichtlich der Quellenauswahl und des Erkenntnisprozesses führt, Interessen gefährdet werden, die durch die Due-Process-Klauseln des Fünften und 14. Zusatzartikels geschützt sind.[343]

Nach diesen dürfen den Bürgern weder auf gesamtstaatlicher (Fünfter Zusatzartikel) noch auf bundesstaatlicher Ebene (14. Zusatzartikel) Leben, Freiheit oder Eigentum ohne Einhaltung des Rechtsstaatsprinzips (Due Process of Law) genommen

---

[339] Siehe oben Kapitel 3,C.I.2.b).

[340] Siehe oben Kapitel 3,C.I.2.c).

[341] Siehe oben Kapitel 3,C.I.2.d).

[342] Siehe oben Kapitel 3,C.I.2.e).

[343] Eine aktuelle Untersuchung des Privatheitsschutzes durch die Due Process-Klauseln liefert auch: *Wittmann*, Der Schutz der Privatsphäre vor staatlichen Überwachungsmaßnahmen durch die US-amerikanische Bundesverfassung, 2014, 41 ff.

werden. Je nachdem, ob die betroffenen Interessen Anerkennung als Fundamental Right gefunden haben oder nicht, kommen unterschiedliche Rechtfertigungsanforderungen an Eingriffe zum Tragen. Eingriffe in Fundamental Rights erfordern substanzielle Rechtsstaatlichkeit (Substantive Due Process), während anderweitige Eingriffe lediglich prozessuale Rechtsstaatlichkeit (Procedural Due Process) erfüllen müssen.

Teilaspekte der Privatheit genießen ein erhöhtes Schutzniveau als (Fundamental) Right to Privacy (siehe a)). Soweit bestimmten Sachverhalten jedoch nicht ausdrücklich dieser Stellenwert zuerkannt wurde, finden sie nur Schutz durch prozessuale Rechtsstaatlichkeit (siehe b)). Zu klären ist, welchen Stellenwert die Verfassung dem durch informationelle Preisgabe drohenden Kontrollverlust über die eigenen Daten zumisst (siehe c))

a) (Fundamental) Right to Privacy

Nach dem Fünften und 14. Zusatzartikel wird denjenigen nicht explizit genannten Rechten der Status als Fundamental Right gewährt, die „implicit in the concept of ordered liberty“ sind.[344] Dies sind insbesondere die Rechte, die „deeply rooted in this Nation’s history and tradition“ sind.[345] Eingriffe bedürfen substanzieller Rechtsstaatlichkeit, werden also der strengen Rechtfertigungsprüfung nach der sogenannten Strict Scrutiny unterzogen. Zur Rechtfertigung muss dann ein zwingender staatlicher Zweck vorliegen, der nicht auch durch weniger restriktive Mittel gleich wirksam erreicht werden kann.[346]

Ein solches Fundamental Right ist das Right to Privacy. Es entsteht aus dem Zusammenspiel des Fünften und 14. Zusatzartikels mit anderen Zusatzartikeln. Diese kreieren „penumbras“, also Halbschatten, unter denen bestimmte Aspekte von Privatheit Schutz finden.[347] Dies ist nach wie vor Stand der Rechtsprechung, auch wenn sich *Justice Scalia* jüngst drastisch ablehnend äußerte: „a generalized right of privacy that comes from penumbras and emanations, blah blah blah, garbage“.[348]

Inhaltlich ist der Schutzbereich des Right to Privacy nicht eindeutig definiert. *Thomsons* Feststellung aus dem Jahr 1975: „Perhaps the most striking thing about the right to privacy is that nobody seems to have any very clear idea what it is“[349], ist auch heute noch nicht überholt.

Anerkannterweise geschützt ist die „independence in making certain kinds of important decisions“, also die Freiheit, über persönliche Angelegenheiten selbst zu

344 Palko v. State of Connecticut, 302 U.S. 319, 325 (1937).
345 Moore v. City of East Cleveland, Ohio, 431 U.S. 494, 503 (1977).
346 Die Idee der Strict Scrutiny geht zurück auf: United States v. Carolene Products Co., 304 U.S. 144, 152, Fn. 4 (1938).
347 Griswold v. Connecticut, 381 U.S. 479, 484 (1965).
348 Zitiert nach: *Barakat*, Scalia Expects NSA Program to End Up in Court 25.9.2013.
349 *Thomson*, The Right to Privacy, 4 Philosophy & Public Affairs (1975), 295, 295; vgl.: 312.

entscheiden.[350] Der Schutzgegenstand ist vergleichbar mit der von *Rössler* beschriebenen dezisionalen Privatheit.[351] Das Right to Privacy schützt unter anderem Eheschließungen zwischen Menschen unterschiedlicher Hautfarbe,[352] die Entscheidung zur Verwendung von Verhütungsmitteln,[353] die Entscheidung zur Verwendung von Verhütungsmitteln durch unverheiratete Paare,[354] das Recht zum Schwangerschaftsabbruch,[355] das Praktizieren gleichgeschlechtlichen Geschlechtsverkehrs,[356] die Entscheidung, selbst über die eigene Haarlänge zu entscheiden,[357] vor der Pflicht zu übermäßig langem unbezahlten Mutterschutz[358] und vor chirurgischen Untersuchungen.[359] Umstritten ist, ob Kranken das Recht gewährleistet wird, auf Behandlungsmethoden zurückzugreifen, deren Wirksamkeit (noch) nicht belegt ist.[360]

Uneinigkeit besteht darüber, inwieweit informationelle Privatheit durch das Right to Privacy geschützt wird. Ausdrücklich anerkannt wurde der Schutz informationeller Privatheit als Fundamental Right nur in sehr wenigen Fällen. Wegbereiter war die U.S.-Supreme-Court-Entscheidung Whalen v. Roe, in der das grundsätzliche Bestehen des Privacy-Schutzes am „individual interest in avoiding disclosure of personal matters“ anerkannt wurde (wenngleich im konkreten Fall verneint).[361] Die Argumentation wird aufgegriffen, ihre Einschlägigkeit aber abgelehnt in Paul v. Davis. Im zugrunde liegenden Fall verteilten Polizeibeamte Handzettel in Läden, die Namen und Fotos von Ladendieben zeigten mit dem Vermerk „Active Shoplif-

---

[350] Whalen v. Roe, 429 U.S. 589, 599 f. (1977); ausführlich: *Solove/Schwartz*, Information Privacy Law, ^{3}2009, 447 ff.

[351] Siehe oben Kapitel 2,A.II; diese Parallele zieht auch: *Hornung*, Grundrechtsinnovationen, 2015, 276, Fn. 405.

[352] Loving v. Virginia, 388 U.S. 1 (1967).

[353] Griswold v. Connecticut, 381 U.S. 479 (1965).

[354] Eisenstadt v. Baird, 405 U.S. 438 (1972).

[355] Roe v. Wade, 410 U.S. 113 (1973) und Planned Parenthood of Southeastern Pennsylvania v. Casey, 505 U.S. 833 (1992).

[356] Lawrence v. Texas, 539 U.S. 558 (2003). Anders noch die Rechtslage in Virginia im Jahr 1975, als gleichgeschlechtlicher Geschlechtsverkehr zur Verhinderung moralischer Verbrechen verboten werden durfte: „the State is not required to show that moral delinquency actually results from homosexuality. It is enough for upholding the legislation to establish that the conduct is likely to end in a contribution to moral delinquency.“: Doe v. Commonwealth's Attorney for City of Richmond, 403 F.Supp. 1199, 1202 (E.D. Va. 1975); aufrechterhalten durch: Doe v. Commonwealth's Attorney for City of Richmond, 425 U.S. 901 (1976).

[357] Kelley v. Johnson, 425 U.S. 238, 250 ff. (1976) (*Marshall*, *Brennan*, *JJ*., dissenting) und Stull v. School Bd. of Western Beaver Junior-Senior High School, 459 F.2d 339, 347 f. (3d Cir. 1972); zum Right to Privacy der Alaska-Verfassung: Breese v. Smith, 501 P.2d 159, 169 (Alaska 1972).

[358] Cleveland Board of Education v. LaFleur, 414 U.S. 632 (1974).

[359] „No right is held more sacred or is more carefully guarded by the common law than the right of every individual to the possession and control of his own person, free from all restraint or interference of others unless by clear and unquestionable authority of law.“: Union Pacific Railway v. Botsford, 141 U.S. 250, 251 (1891).

[360] Bejahend: Rutherford v. United States, 438 F.Supp. 1287, 1300 (W.D. Okla. 1977) und Suenram v. Society Valley Hospital, 383 A.2d 143, 148 (N.J. Super.L. 1977); ablehnend: People v. Privitera, 591 P.2d 919 (en banc 1979).

[361] Whalen v. Roe, 429 U.S. 589, 599 (1977).

ters".[362] Auch in diese Reihe fällt die U.S.-Supreme-Court-Entscheidung Nixon v. Administrator of General Services, in der ein Privacy-Interesse Präsident *Nixons* an Aufzeichnungen über seine Kommunikation mit seiner Familie anerkannt wird.[363] In diese Richtung geht der U.S. Supreme Court schließlich ebenfalls, wenn er die Pflicht, eine beabsichtigte Abtreibung vorab dem Ehemann mitzuteilen, für verfassungswidrig erklärt, da die Frau aus Angst vor gewalttätiger Reaktion des Ehemannes von der Abtreibung abgehalten werden könnte.[364]

Umstritten ist, ob informationelle Privatheit über diese ausdrücklich anerkannten Fälle hinaus Schutz als Fundamental Right erfährt. Das Right to Informational Privacy findet keine ausdrückliche Erwähnung im US-Verfassungsrecht. Einige Landesverfassungen erkennen zwar Rights to Privacy/Rights of Privacy an: Alaska (Art. I, § 22), Arizona (Art. II, § 8), Florida (Art. I, § 23), Hawaii (Art. I, § 6 f.), Illinois (Art. I, § 6), Kalifornien (Art. I, § 1), Louisiana (Art. I, § 5), Montana (Art. II, § 10), South Carolina (Art. 1, § 10) und Washington (Art. I, § 7). Deren Konturen sind jedoch im Wesentlichen unbestimmt: In der Praxis kommt ihnen, abgesehen von dem kalifornischen Privacy-Recht, bislang keine große Bedeutung zu.[365]

Gerade die Abneigung der US-Gerichte gegen die teleologische Auslegungsmethode macht das Right to Informational Privacy besonders schwer begründbar.[366] In der Konsequenz sind sie sehr zögerlich mit seiner Annahme. Zwar fand das Right to Informational Privacy Anerkennung durch fast alle Circuit Courts.[367] Eine ständige Rechtsprechung, die dieses Recht bejahen und ihm Konturen verleihen würde, besteht allerdings nur begrenzt. Die Frustration über diesen Zustand wird deutlich in einer der Dissenting Opinions in Nelson v. National Aeronautics and Space Admin.: „Is there a constitutional right to informational privacy? Thirty-two Terms ago, the Supreme Court hinted that there might be and has never said another word about it. With no Supreme Court guidance except this opaque fragment, the courts of appe-

---

[362] Paul v. Davis, 424 U.S. 693, 712 f. (1976).

[363] Nixon v. Administrator of General Services, 433 U.S. 425, 427 (1977).

[364] Planned Parenthood of Southeastern Pennsylvania v. Casey, 505 U.S. 833, 893 (1992). Da das Gericht die Notwendigkeit für den Privatheitsschutz in dieser Entscheidung auf die Überlegung stützt, dass mangelnde Privatheit zur Einschüchterung führen kann und damit die Entschließungsfreiheit beeinträchtigt, könnte das Urteil auch der eben angesprochenen Kategorie des Schutzes der dezisionalen Privatheit zugeordnet werden.

[365] *Buchner*, Informationelle Selbstbestimmung im Privatrecht, 2006, 9. Der Privatheitsschutz der kalifornischen Verfassung wirkt auch zwischen Privaten, st. Rspr., statt vieler: Hill v. National Collegiate Athletic Assn., 865 P.2d 633, 644 (Cal. 1994).

[366] So auch: *Lange*, Grundrechtsbindung des Gesetzgebers, 2010, 49.

[367] Barry v. City of New York, 712 F.2d 1554, 1559 (2d Cir. 1983); United States v. Westinghouse Electric Corp., 638 F.2d 570, 577–580 (3d Cir. 1980); Walls v. City of Petersburg, 895 F.2d 188, 192 (4th Cir. 1990); Plante v. Gonzalez, 575 F.2d 1119, 1132, 1134 (5th Cir. 1978); J.P. v. DeSanti, 653 F.2d 1080, 1090 (6th Cir. 1981) (In dieser Entscheidung stellt der Sechste Circuit Court jedoch fest, dass er zunächst keine Ausdehnung des Rights to Informational Privacy über die in Whalen und Nixon festgestellten Sachverhalte hinaus vornehmen wird); Bloch v. Ribar, 156 F.3d 673, 684 (6th Cir. 1998) (ebenfalls restriktiv); Kimberlin v. United States Department of Justice, 788 F.2d 434 (7th Cir. 1986) und In re Crawford, 194 F.3d 954, 959 (9th Cir. 1999).

als have been left to develop the contours of this free-floating privacy guarantee on their own. It's a bit like building a dinosaur from a jawbone or a skull fragment, and the result looks more like a turducken." (also einem Braten aus Truthahn, Ente und Hühnchen).[368]

Derzeit wird man davon ausgehen müssen, dass Privatheitsaspekte, denen nicht ausdrücklich der Status als Fundamental Right zugeordnet wurde, diesen Status auch nicht besitzen und damit keinen substanziellen Due-Process-Schutz genießen.

b) Prozessualer Due-Process-Schutz

Wie gesehen ist nicht jeder Aspekt von Privatheit zugleich als Teil des Rights to Privacy anerkannt. Nicht erfasst sind weiter beispielsweise ein Recht auf Sterbehilfe,[369] ein Recht zur Prostitution in den eigenen vier Wänden[370] und ein Recht auf Marihuana-Konsum.[371] Bereiche, für die es an der Anerkennung fehlt, erfahren aber ebenfalls Schutz durch die Due-Process-Klauseln. Zur Anwendung kommt lediglich prozessualer Due-Process-Schutz, sodass die Interessen nach dem sogenannten Rational-Basis-Test einschränkbar sind. Damit müssen sie lediglich in einem nachvollziehbaren Verhältnis zu einem legitimen Zweck stehen.[372] Die Beweislast dafür, dass dies nicht der Fall ist, liegt bei demjenigen, der die Verletzung des Rechtsstaatlichkeitsprinzips behauptet.[373]

Dieses niedrige Schutzniveau möchten zahlreiche Stimmen in der Literatur anheben, sei es auch nur durch Ausdehnung des einfachrechtlichen Schutzes informationeller Privatheit.[374] Auf die verfassungsrechtliche Einordnung bleiben diese rechtspolitischen Forderungen jedoch ohne Auswirkungen.

c) Anwendung auf den konkreten Fall

Informationelle Preisgabe kann dazu führen, dass Nutzer auf lange Sicht gesehen nicht mehr über die Preisgabe und Verwendung ihrer personenbezogenen Daten

---

[368] Nelson v. National Aeronautics and Space Admin., 568 F.3d 1028, 1052 (9th Cir. 2009) (*Kozinski*, *CJ.*, *Kleinfeld*, *Bea*, *JJ.*, dissenting).

[369] Washington v. Glucksberg, 521 U.S. 702 (1997).

[370] Zum Right to Privacy der Hawaii-Verfassung: State v. Mueller, 671 P.2d 1351, 1359 (Hawaii 1983).

[371] State v. Kantner, 493 P.2d 306, 310 (Hawaii 1972). Etwas anderes gilt für den Marihuana-Besitz und Genuss in den eigenen vier Wänden in Alaska: Ravin v. State, 537 P.2d 494, 504 (Alaska 1975).

[372] Der Rational-Basis-Test geht zurück auf: United States v. Carolene Products Co., 304 U.S. 144, 152 (1938).

[373] United States v. Carolene Products Co., 304 U.S. 144, 152 (1938).

[374] *Nehf*, Recognizing the Societal Value in Information Privacy, 78 Washington L. Rev. (2003), 1, 6 und *Schwartz*, The Computer in German and American Constitutional Law, 37 American J. of Comparative L. (1989), 675, 677. Ein Plädoyer für die Einführung expliziten verfassungsrechtlichen Schutzes des Rights to Informational Privacy liefert: *Lin*, Prioritizing Privacy, 17 Berkeley Tech. L.J. (2002), 1085 ff. Forderungen nach einfachrechtlichem Schutz finden sich u.a. in: *The White House*, Consumer Data Privacy in a Networked World, 2.2012, 35 f.

bestimmen können und in der Folge Selbstzensur hinsichtlich der Quellenauswahl und des Erkenntnisprozesses üben. Doch erscheint es zweifelhaft, ob das Right to Privacy vor diesem Kontrollverlust schützt. Ist dies der Fall, besteht hoher substanzieller Due-Process-Schutz. Andernfalls besteht nur niedriger prozessualer Due-Process-Schutz, sodass Eingriffe bei Vorliegen irgendeines rationalen Zwecks gerechtfertigt werden können.

Einen ausdrücklichen Schutz vor der Ausspähung von Internetaktivitäten gewährleistet das Right to Privacy bislang nicht. Zudem wird vorgeschlagen, die Grundsätze der beim Vierten Zusatzartikel geltenden Third-Party-Doktrin[375] auf das Right to Privacy auszudehnen. So argumentiert die angesprochene Dissenting Opinion in Nelson v. National Aeronautics and Space Admin. restriktiv: „But one's privacy interest ought to wane the more widely the information is known. […] Does one really have a free-standing constitutional right to withhold from the government information that others in the community are aware of? I don't think so. How then can it be constitutionally impermissible for the government to ask a subject's friends, family and neighbors what they know about him? Surely there's no constitutional right to have the state be the last to know."[376] Würde dies geschehen, müssten Internetaktivitäten wohl wie auch unter dem Vierten Zusatzartikel als beinahe schutzlos gewertet werden, da sie Datenübertragung an Dritte beinhalten.

Teilaspekte informationeller Privatheit genießen den Status eines Fundamental Rights. Bislang wurde jedoch in keinem Präzedenzfall festgestellt, dass ein Recht, im Internet selbst bestimmen zu können, wann und innerhalb welcher Grenzen persönliche Sachverhalte offenbart werden, dem Right to Informational Privacy zuzurechnen ist. Selbst wenn dieser Kontrollverlust also nicht durch die Nutzer, sondern durch staatliche Stellen herbeigeführt würde, bestünde entweder schon kein Schutz als Fundamental Right oder dieser Schutz würde durch eine entsprechende Anwendung der Third-Party-Doktrin ausgeschlossen. Es bestünde damit nur ein geringes Schutzniveau, die staatlichen Eingriffe wären nach dem Rational-Basis-Test rechtfertigbar.

Doch wenn schon nur geringer Schutz gegen staatliche Eingriffe in die informationelle Privatheit im Internet besteht, gilt dies erst recht, wenn die Bedrohungen von den Nutzern selbst ausgehen. Dem Schutz Privater vor dem Kontrollverlust über ihre Daten wird daher in der Verfassung nur sehr begrenzte Bedeutung zugemessen. Ein verfassungsrechtliches Interesse an der Verhinderung informationeller Preisgabe zu dem Zweck, Nutzern die Möglichkeit zu geben zu wissen, wer wann was über sie weiß, ist daher beinahe nicht existent.

---

[375] Siehe oben Kapitel 3,C.I.2.d).

[376] Nelson v. National Aeronautics and Space Admin., 568 F.3d 1028, 1053 (2009) (*Kozinski*, *CJ.*, *Kleinfeld*, *Bea*, *JJ.*, dissenting).

4. Informationsfreiheit

Weiter könnte die Informationsfreiheit berührt sein, wenn informationelle Preisgabe dazu führt, dass eine neutrale Quellenauswahl der Nutzer beeinträchtigt wird und diese zudem durch Selbstzensur vom Aufrufen kontroverser Quellen abgehalten werden.

Das Recht, sich ungehindert zu informieren, wird durch die Redefreiheit nach dem Ersten Zusatzartikel geschützt. Nach diesem darf der Kongress[377] kein Gesetz erlassen, das die Redefreiheit verkürzt. Dabei wird die Redefreiheit weit ausgelegt und umfasst auch das Recht zur ungehinderten Information als Vorbedingung der Rede. Der U.S. Supreme Court führt aus: „If the First Amendment means anything, it means that a State has no business telling a man, sitting alone in his own house, what books he may read or what films he may watch. Our whole constitutional heritage rebels at the thought of giving government the power to control men's minds."[378] Einschränkungen unterliegen regelmäßig den strengsten Rechtfertigungsanforderungen, der Strict Scrutiny.

Auch das Recht, sich ohne Einflussnahme und uneingeschüchtert im Internet informieren zu können, ist vom Ersten Zusatzartikel zur US-Verfassung umfasst.[379] Während die durch informationelle Preisgabe entstehenden Gefahren, wenn überhaupt, nur in sehr geringem Maße verfassungsrechtlich geschützte Privatheitsinteressen berühren, tangieren sie jedenfalls durch die Informationsfreiheit geschützte Belange der Einzelpersonen.

II. Allgemeinwohlbelange

Schließlich könnten die durch informationelle Preisgabe gefährdeten Allgemeinwohlbelange verfassungsrechtlichen Stellenwert besitzen. Gerade in der jüngeren US-Literatur wird – in Übernahme europäischer und deutscher Überlegungen – betont, dass durch den Verlust informationeller Privatheit auch Konsequenzen für rechtlich zu schützende Allgemeinwohlbelange entstehen können. Dazu wird informationeller Privatheit über den Schutz der Individualinteressen hinaus der Zweck zugeschrieben, die Persönlichkeitsentfaltung innerhalb der Gemeinschaft und die gesellschaftliche Entwicklung als solche zu schützen. Gerade weil der verfassungsrechtliche Schutz der informationellen Privatheit in den USA hinter dem in anderen Rechtsordnungen, beispielsweise der deutschen, zurückbleibt, bedarf es der ausführlichen Herleitung des gesellschaftlichen Werts der informationellen Privatheit.

Wiederum kann unterteilt werden in den Schutz der informationellen Privatheit Dritter (siehe 1.), den Schutz des gesellschaftlichen Fortschritts (siehe 2.) und den Schutz der Demokratie (siehe 3.).

---

377 Der Erste Zusatzartikel findet über den 14. Zusatzartikel Anwendung auf die Bundesstaaten: Gitlow v. People of State of New York, 268 U.S. 652, 666 (1925).

378 Stanley v. Georgia, 394 U.S. 557, 565 (1969).

379 *Cohen*, DRM and Privacy, 18 Berkeley Tech. L. J. (2003), 575, 591.

1. Informationelle Privatheit Dritter

Die durch informationelle Preisgabe bedrohte informationelle Privatheit Dritter könnte verfassungsrechtlichen Stellenwert genießen.

Veröffentlichen die Preisgebenden personenbezogene Daten Dritter, die sie ohne Zutun der Dritten erhalten haben, ohne oder gegen deren Willen, haben die Dritten eine berechtigte Privatheitserwartung, sodass der Vierte Zusatzartikel jedenfalls Schutz vor staatlichen Zugriffen auf die Daten bieten würde. Ein verfassungsrechtlich geschütztes Interesse an der Privatheitswahrung der Dritten in diesen Fällen liegt daher vor.

Zudem führt die Preisgabe von Daten, die auch Dritte betreffen, dazu, dass deren „individual interest in avoiding disclosure of personal matters“[380] und damit deren Right to Informational Privacy berührt werden.

Weil in den Fällen, in denen die Preisgabe durch Andere als die Rechtsträger selbst erfolgt, die Third-Party-Doktrin häufig keine Anwendung findet, greift dann der volle Schutz. Wollte der Staat auf Dritte betreffende Daten Zugriff nehmen, die Andere ohne Zutun der Dritten preisgegeben haben, müsste er die Hürde des Vierten Zusatzartikels beziehungsweise des Rights to Informational Privacy überwinden. Dieses hohe Schutzniveau, das die Verfassung der informationellen Privatheit Dritter zuerkennt, ist daher auch bei der Untersuchung staatlicher Möglichkeiten zur Verhinderung informationeller Preisgabe zu berücksichtigen.

2. Gesellschaftlicher Fortschritt

Weiter könnte der durch informationelle Preisgabe gefährdete gesellschaftliche Fortschritt ein verfassungsrechtlich geschütztes Interesse darstellen.

Ihm wird mittelbar durch den Ersten Zusatzartikel Rechnung getragen, der die Entstehung neuer Ideen als Grundlage der Redefreiheit schützt. Prägend ist das Konzept des sogenannten Marktplatzes der Ideen, auf dem sich alle möglichen Ideen gegeneinander durchsetzen müssen, um so gesellschaftlichen Fortschritt zu erreichen.[381] Gewinnerin ist die Idee, die die Audienz überzeugen kann. Da die Wahrheit nicht mit Sicherheit bekannt ist („No one has a pipeline to ultimate reality“[382]), können nur so neue, relativ wahre Ansichten entwickelt werden. Der umkämpfte Prozess der Überzeugungsfindung gerät aus dem Gleichgewicht, wenn mögliche Konkurrenten – in Gestalt von unliebsamen oder abweichenden Ideen – vorab ausgeschlossen werden. Dieses Problem wird dadurch verstärkt, dass weiterführende, aber kritische Ideen sehr leicht gegen populäre ausgetauscht werden können, ohne

---

[380] Whalen v. Roe, 429 U.S. 589, 599 (1977).

[381] In die US-Rechtsprechung eingeführt durch: Abrams v. United States, 250 U.S. 616, 630 (1919) (*Holmes*, *J.*, dissenting): „the best test of truth is the power of the thought to get itself accepted in the competition of the market“; vgl.: *Mill*, Über die Freiheit, 2010 (Original: 1859), 59, 77 und *Posner*, Economic Analysis of Law, [7]2007, 727 f.

[382] *Posner*, Economic Analysis of Law, [7]2007, 727.

dass dies den Marktteilnehmern bewusst wird. Eine Hemmung des gesellschaftlichen Fortschritts würde so die gemäß dem Ersten Zusatzartikel geschützte Ideenfreiheit tangieren.

Ergänzend belegt bereits der Verfassungswortlaut die Bedeutung gesellschaftlichen Fortschritts für das US-Rechts- und Gesellschaftssystem. Die US-Verfassung ist deutlich stärker auf die bloße Kompetenzverteilung zwischen den Staaten und dem Bundesgesetzgeber ausgerichtet als es das Grundgesetz ist: In ihr finden sich daher, bedingt durch den begrenzteren Regelungsgegenstand der Verfassung, weniger Hinweise auf den Stellenwert gesellschaftlichen Fortschritts als im Grundgesetz. Dennoch zeigt schon die Präambel, dass die Verfassung dem Zweck dient, das Gemeinwohl und damit mittelbar den gesellschaftlichen Fortschritt zu unterstützen. Art. 1 Sec. 8 weist dem Kongress die Gesetzgebungskompetenz zu, für das Gemeinwohl zu sorgen (Abs. 1) und den Fortschritt von Wissenschaft und nützlicher Kunst durch die Sicherung geistigen Eigentums zu fördern (Abs. 8). Die weitere Ausgestaltung gesellschaftlichen Lebens bleibt dann den Bundesstaaten überlassen.

Auch der durch informationelle Preisgabe bedrohte gesellschaftliche Fortschritt genießt somit Verfassungsrang. Jedoch handelt es sich bei dem Ziel der Gewährleistung gesellschaftlichen Fortschritts um ein abstraktes Ziel, aus dem keine individuellen Handlungs- oder Unterlassungspflichten erwachsen.

3. Demokratie

Schließlich könnte es ein verfassungsrechtlich geschütztes Interesse am Gedeihen der Demokratie geben, das beeinträchtigt wird, wenn informationelle Preisgabe dazu führt, dass Nutzer die Möglichkeit zum Erkennen notwendiger Veränderungen verlieren, die zur politischen Teilnahme erforderliche Selbstbestimmtheit einbüßen oder von politischer Partizipation abgeschreckt werden.

Der durch die Informationsfreiheit nach dem Ersten Zusatzartikel geschützte ungehinderte Zugang zu Informationen ist Basis der Demokratie, wie auch die folgenden Formulierungen des U.S. Supreme Courts zeigen: „[T]he First Amendment embodies more than a commitment to free expression and communicative interchange for their own sakes; it has a *structural* role to play in securing and fostering our republican system of self-government. Implicit in this structural role is not only the principle that debate on public issues should be uninhibited, robust, and wide-open, but also the antecedent assumption that valuable public debate – as well as other civic behavior – must be informed. The structural model links the First Amendment to that process of communication necessary for a democracy to survive, and thus entails solicitude not only for communication itself, but also for the indispensable conditions of meaningful communication.“[383] Werden Nutzer durch personalisierte Informationsangebote in eine Richtung gelenkt und verlieren dadurch die Möglich-

[383] Richmond Newspapers, Inc. v. Virginia, 448 U.S. 555, 587 f. (1980) (Hervorhebung im Original).

keit zum Erkennen notwendiger Veränderungen,[384] ist damit die Informationsfreiheit in ihrer Funktion als Grundlage der Demokratie betroffen.

Weiter beruht ein funktionierender öffentlicher Diskurs auf der Selbstbestimmtheit der Akteure, wie der U.S. Supreme Court darlegt: „The First Amendment mandates that we presume that speakers, not the government, know best both what they want to say and how to say it. […] To this end, the government, even with the purest of motives, may not substitute its judgment as to how best to speak for that of speakers and listeners; free and robust debate cannot thrive if directed by the government."[385] Werden Nutzer durch informationelle Preisgabe in ihrer Selbstbestimmtheit beeinträchtigt,[386] wird dadurch die durch den Ersten Zusatzartikel geschützte Redefreiheit berührt.

Zudem anerkennt der U.S. Supreme Court den Zusammenhang zwischen der durch die Abschreckung von politischer Teilnahme[387] bedrohten Meinungsfreiheit und dem Gelingen demokratischer Prozesse, wenn er feststellt, dass in bestimmten Fällen auch eine anonyme öffentliche Meinungsäußerung zulässig sein muss, da „identification and fear of reprisal might deter perfectly peaceful discussions of public matters of importance."[388]

Weiter sieht der U.S. Supreme Court auch generell das Aufrechterhalten eines stabilen politischen Systems in ständiger Rechtsprechung als unzweifelhaft zwingenden staatlichen Zweck an.[389]

Schließlich kann wiederum der Verfassungswortlaut als Beleg dafür dienen, dass der Demokratie ein hoher Stellenwert zukommt: Art. 1 Sec. 2 para. 1 und Sec. 2 des 14. Zusatzartikels regeln die Wahl der Representatives, Art. 1 Sec. 2 para. 5 deren Amtsenthebung. Art. 1 Sec. 3 para. 1 und der 17. Zusatzartikel regeln die Wahl der Senatoren, Art. 1 Sec. 3 para. 6 und 7 deren Amtsenthebung. Art. 1 Sec. 4 bestimmt die Details der Wahlen. Art. 2 Sec. 1 und der zwölfte Zusatzartikel regeln die Wahl des Präsidenten, der 22. Zusatzartikel seine maximale Amtszeit. Art. 2 Sec. 4 regelt die Möglichkeit der Amtsenthebung des Präsidenten und anderer hoher Beamter. Gemäß dem 15. und 19. Zusatzartikel werden Wahlrechte nicht durch Hautfarbe oder Geschlecht beeinträchtigt. Die Demokratie ist damit ein verfassungsrechtlich geschütztes Interesse. Jedoch konstituiert auch das US-Verfassungsrecht gerade keine Pflicht zur Mitwirkung an der Demokratie.

---

384 Siehe oben Kapitel 3,A.III.3.a).

385 Riley v. National Federation of the Blind of North Carolina, Inc., 487 U.S. 781, 791 (1988).

386 Siehe oben Kapitel 3,A.III.3.b).

387 Siehe oben Kapitel 3,A.III.3.c).

388 Talley v. California, 362 U.S. 60, 65 (1960).

389 St. Rspr., statt vieler: Storer v. Brown, 415 U.S. 724, 736 (1974) und Eu v. San Francisco County Democratic Cent. Committee, 489 U.S. 214, 226 (1989).

D. Vergleich

Im Rahmen eines funktionalen Rechtsvergleichs[390] wird untersucht, welche Lösungen die deutsche und die US-amerikanische Verfassungsordnung bieten, um den Gefahren informationeller Preisgabe zu begegnen. Dabei werden im Folgenden nicht nur die verfassungsrechtlichen Gewährleistungsgehalte der betroffenen Rechte untersucht, sondern auch ein Vergleich zwischen den zugrunde liegenden Verfassungs- und Gesellschaftstraditionen gezogen.

I. Evaluationsmaßstäbe

Im Rahmen der Analyse, welche faktischen Gefahren durch informationelle Preisgabe entstehen können und welche Rechtsgüter dadurch jeweils nach deutschem und US-amerikanischem Verfassungsrecht bedroht werden, wurde der Grundstein zur Beantwortung der Fragen gelegt, ob eine Pflicht zum Schutz dieser Güter besteht[391] beziehungsweise ob die informationelle Preisgabe zum Schutz dieser Güter verhindert werden darf.[392] Informationelle Preisgabe birgt Gefahren für Interessen, die sowohl in Deutschland als auch in den USA verfassungsrechtlichen Schutz genießen. Dabei kommt der Verhinderung der Bedrohungen insbesondere Bedeutung zu, wenn die gefährdeten Rechtsgüter verfassungsrechtlich geschützt sind.

1. Rechtsgüter der Preisgebenden

Durch informationelle Preisgabe können sowohl die informationelle Privatheit der Preisgebenden als auch deren Informationsfreiheit beeinträchtigt werden.

Zunächst können Nutzer durch informationelle Preisgabe langfristig ihre informationelle Privatheit einbüßen und in der Folge Selbstzensur hinsichtlich der Quellenauswahl und des Erkenntnisprozesses üben. Im deutschen (Art. 2 Abs. 1 in Verbindung mit Art. 1 Abs. 1 GG) und im europäischen Recht (Art. 7 und 8 GR-Ch, Art. 8 EMRK) kommt der informationellen Privatheit der Nutzer ein hoher Rang zu. Dabei tangiert schon eine bloße Angst davor, infolge informationeller Preisgabe die Kontrolle über die eigenen Daten zu verlieren und Überwachung ausgesetzt zu sein, die geschützten Interessen am Erhalt der informationellen Privatheit.

In den Vereinigten Staaten erfährt die informationelle Privatheit grundsätzlich Schutz durch den Vierten Zusatzartikel sowie die Due-Process-Klauseln. Jedoch greift der Schutz des Vierten Zusatzartikels neben anderen Einschränkungen jeden-

---

[390] Generell zur Methodik der Rechtsvergleichung: *Constantinesco*, Rechtsvergleichung, 1971, 204 ff.; *Rabel*, Aufgabe und Notwendigkeit der Rechtsvergleichung, 1925, 2 ff.; *Rheinstein*, Einführung in die Rechtsvergleichung, 1974, 16 ff.; *Sacco*, Einführung in die Rechtsvergleichung, 2001, 13 ff.; *Wieser*, Vergleichendes Verfassungsrecht, 2005, 16 ff.; sowie der historisch bis 1900 zurückreichende Sammelband *Zweigert/Puttfarken* (Hrsg.), Rechtsvergleichung 1978; zur funktionalen Methode: *Wieser*, Vergleichendes Verfassungsrecht, 2005, 20.

[391] Siehe unten Kapitel 5.

[392] Siehe unten Kapitel 6.

falls gemäß der Third-Party-Doktrin nicht, sobald die Preisgebenden ihre Daten irgendjemandem anvertraut haben. Da Preisgabe im Internet schon technisch voraussetzt, dass Daten an andere Menschen oder Geräte übermittelt werden, bietet der Vierte Zusatzartikel regelmäßig keinen Schutz. Weiter kann die informationelle Privatheit durch die Due-Process-Klauseln abgesichert werden. In eng begrenzten Fällen wurde ein Recht auf informationelle Privatheit als Fundamental Right anerkannt, sodass es nur unter Wahrung sogenannter substanzieller Rechtsstaatlichkeit eingeschränkt werden kann. Diese Fälle sind jedoch nicht verallgemeinerungsfähig. Zudem wird sogar diskutiert, die Third-Party-Doktrin auch auf das Right to Informational Privacy zu übertragen und damit den Schutz durch das substanzielle Rechtsstaatlichkeitsgebot entfallen zu lassen, wenn die Daten irgendeinem Dritten anvertraut werden. Regelmäßig erfährt informationelle Privatheit in den USA daher nur minimalen Schutz durch das allgemeine prozessuale Rechtsstaatlichkeitsgebot. Es ist daher davon auszugehen, dass der informationellen Privatheit der Preisgebenden in der US-Verfassung nach derzeitiger Auslegung kein hoher Stellenwert zugemessen wird. Die Rede ist zurecht von einem „nicht nur für den deutschen Rechtsanwender erschreckenden Befund“.[393] Selbst wenn die befürchteten Gefahren nicht durch Private, sondern direkt durch den Staat ausgelöst würden, ist anzunehmen, dass kein verfassungsrechtlicher Schutz gegen sie bestünde.

Weiter kann informationelle Preisgabe dazu führen, dass Nutzern keine neutrale Quellenauswahl zur Verfügung steht oder sie vor dem Aufrufen kontroverser Quellen zurückschrecken. Dadurch werden Interessen gefährdet, die durch die Informationsfreiheit der Preisgebenden geschützt sind. Die Informationsfreiheit im Sinne des Grundgesetzes (Art. 5 Abs. 1 Satz 1 Halbsatz 2 GG) und ihre europarechtlichen Pendants (Art. 10 Abs. 1 Satz 2, 2. Alt. EMRK; Art. 11 Abs. 1 Satz 2, 2. Alt. GR-Ch) schützen die Nutzer davor, durch den Staat von dem ungehinderten Zugang zu Informationen abgehalten zu werden. Werden die Nutzer durch eine Vorselektion der Quellen oder durch Selbstzensur hinsichtlich der Quellenauswahl am freien Zugang zu Informationen gehindert, werden damit Interessen berührt, die durch die Informationsfreiheit geschützt sind. Sind Grundrechte verschiedener Grundrechtsträger in praktische Konkordanz zu bringen, findet in Deutschland regelmäßig eine gleichberechtigte Abwägung zwischen der Informationsfreiheit und den widerstreitenden Interessen statt.

In den Vereinigten Staaten wird das Recht, sich ohne Einflussnahme und uneingeschüchtert im Internet informieren zu können, vom Ersten Zusatzartikel geschützt. Diesem kommt im US-Verfassungssystem eine überragende Bedeutung zu. Bei der Herstellung praktischer Konkordanz setzt er sich regelmäßig gegen alle anderen Belange durch.[394] Damit erfährt die Informationsfreiheit sehr hohen Schutz.

---

[393] Zu dieser Beurteilung kommt *Wittmann* nach Untersuchung des Privatheitsschutzes im US-Verfassungsrecht: *Wittmann*, Der Schutz der Privatsphäre vor staatlichen Überwachungsmaßnahmen durch die US-amerikanische Bundesverfassung, 2014, 370.

[394] Vgl.: *Buchner*, Informationelle Selbstbestimmung im Privatrecht, 2006, 20 ff., 83 ff.; *Post*,

2. Allgemeinwohlbelange

Weiter können durch informationelle Preisgabe Gefahren für die informationelle Privatheit Dritter, für den gesellschaftlichen Fortschritt sowie die Demokratie entstehen.

Betroffen ist zunächst die informationelle Privatheit Dritter, die in Deutschland durch das Recht auf informationelle Selbstbestimmung (Art. 2 Abs. 1 in Verbindung mit Art. 1 Abs. 1 GG) geschützt wird. In den Vereinigten Staaten erfolgt der Schutz durch den Vierten Zusatzartikel beziehungsweise das Right to Privacy.

Weiter kann der gesellschaftliche Fortschritt in seinen drei Teilaspekten kultureller, wissenschaftlicher und wirtschaftlicher Fortschritt bedroht werden, der in beiden Staaten Verfassungsrang genießt.

Schließlich können Risiken für die Demokratie entstehen, wenn die Bürger die Möglichkeit zum Erkennen notwendiger Veränderungen verlieren, aufgrund mangelnder Selbstbestimmung nur eingeschränkt am politischen Prozess teilhaben können oder von politischer Partizipation abgeschreckt werden. Beide Verfassungen schützen vor den drei aufgezählten Gefahren durch individuelle Grundrechte. Zudem anerkennen sie generell den hohen Stellenwert der Demokratie.

II. Analyse

Obwohl die dargestellten Risiken für die deutsche und die US-amerikanische Gesellschaftsordnung gleichermaßen gelten, zeigen sich Unterschiede bei der Analyse, wie stark die Verfassungen die Gefahren missbilligen. Dabei wird aktuell insbesondere in den Vereinigten Staaten ein hitziger Diskurs hinsichtlich des Stellenwerts der informationellen Privatheit geführt. Dieser geht auf ihre sich noch in Entwicklung befindliche rechtliche Absicherung zurück.

1. Rechtsgüter der Preisgebenden

Während der durch die informationelle Preisgabe langfristig entstehende Verlust an informationeller Privatheit im deutschen Verständnis als sehr bedrohlich wahrgenommen wird, bleibt er im US-Verfassungsrecht ohne weitreichende Konsequenzen. Diese abweichende verfassungsrechtliche Bewertung lässt sich vor dem Hintergrund der unterschiedlichen Verfassungs- und Gesellschaftstraditionen begreifen: Die zugrunde liegenden Vorstellungen hinsichtlich der Bedeutung der informationellen Privatheit liegen weit auseinander.[395] Das Recht auf informationelle Selbstbestimmung nach deutschem Verständnis schützt persönliche Würde und individuelle

---

Yellow Press and Privacy, GRUR Int 2006, 283, 292; *Whitman*, The Two Western Cultures of Privacy, 113 Yale L.J. (2004), 1151, 1209 und *Wittern*, Das Verhältnis von Right of Privacy und Persönlichkeitsrecht zur Freiheit der Massenmedien, 2004, 270 ff.

[395] Ausführlich: *Schwartz*, Das Übersetzen im Datenschutzrecht, in: Frank/Maaß/Paul (Hrsg.), Übersetzen, verstehen, Brücken bauen, 1993, Bd. 1, 366, 366 ff; *Hornung*, Grundrechtsinnovationen, 2015, 275 ff.

Selbstentfaltung.[396] Privacy hingegen schützt in den USA als Recht, in Ruhe gelassen zu werden, die Individualinteressen der Einzelnen. Schutzobjekt ist die persönliche Freiheit vor dem Staat, insbesondere im eigenen Heim.[397] Privatheitsschutz dient dabei dem Schutz des Eigentums, nicht der Ehre.[398] Im Vordergrund steht ein ökonomischer Ansatz, nachdem sich auf einem Privatheitsmarkt auch ohne staatliche Intervention ein effizientes Privatheitsschutzniveau herstellen wird.[399]

Untermauert werden die unterschiedlichen Herangehensweisen auch am Beispiel des durch Art. 17 EU-DS-GVO-E ins Spiel gebrachten Rechts auf Vergessenwerden.[400] Es scheint dem europäischen Konsens zu entsprechen, dass sich Privatheitsrechte grundsätzlich gegen die Rechte der verantwortlichen Stellen und das Informationsinteresse der Öffentlichkeit durchsetzen können. Dies wird auch in der Entscheidung des Europäischen Gerichtshofs in Sachen Google v. Costeja González dargelegt.[401] In dem Urteil entschied der Europäische Gerichtshof, dass Art. 7 und 8 GR-Ch bereits jetzt ein Recht gewähren, die Verlinkung auf bestimmte wahre Informationen in einer Suchmaschine verhindern zu lassen. In den Vereinigten Staaten hingegen stößt die Idee eines Rechts auf Vergessenwerden auf große Ablehnung. Teilweise wird es sogar als die größte Gefahr für die Redefreiheit im Internet im kommenden Jahrzehnt bezeichnet und es werden Prophezeiungen angestellt hinsichtlich eines „dramatic clash between European and American conceptions of the proper balance between privacy and free speech, leading to a far less open Internet."[402]

Das, gerade auch im Vergleich zu Deutschland und Europa, niedrige Niveau des Privatheitsschutzes in den Vereinigten Staaten wird vielfach kritisiert.[403] Die dargestellten faktischen Gefahren informationeller Preisgabe[404] – und damit des Verlusts informationeller Privatheit – gelten gleichermaßen in Deutschland und in den Vereinigten Staaten. Während der Zusammenhang zwischen dem Verlust an Privatheit und dem Entstehen der Bedrohungen in Deutschland seit Langem anerkannt ist und entsprechender verfassungs- und einfachrechtlicher Schutz besteht, ist dies in den USA (noch) nicht der Fall. Vielmehr besteht ein signifikantes Grundvertrauen darin, dass der freie Markt das (Privatheits-)Gebaren von Unternehmen kontrolliert.

---

396 *Kang/Buchner*, Privacy in Atlantis, 18 Harvard J. of L. and Tech. (2004), 230 ff. und *Whitman*, The Two Western Cultures of Privacy, 113 Yale L. J. (2004), 1151, 1180 f.

397 *Whitman*, The Two Western Cultures of Privacy, 113 Yale L. J. (2004), 1151, 1211 ff.

398 *Whitman*, The Two Western Cultures of Privacy, 113 Yale L. J. (2004), 1151, 1210.

399 *Kang/Buchner*, Privacy in Atlantis, 18 Harvard J. of L. and Tech. (2004), 230 ff.

400 Dazu: *Ausloss*, The 'Right to be Forgotten', 28 Computer Law & Security Review (2012), 143, 143 ff. und *Hornung/Hofmann*, Ein „Recht auf Vergessenwerden"?, JZ 2013, 163 ff.

401 EuGH EuZW 2014, 541 (546 f.); siehe ausführlich oben Kapitel 3,B.I.1.b).

402 *Rosen*, The Right to be Forgotten, 64 Stanford L. Rev. Online (2012), 88.

403 Statt vieler: *Lin*, Prioritizing Privacy, 17 Berkeley Tech. L. J. (2002), 1085 ff.; *Nehf*, Recognizing the Societal Value in Information Privacy, 78 Washington L. Rev. (2003), 1, 6 und *Schwartz*, The Computer in German and American Constitutional Law, 37 American J. of Comparative L. (1989), 675, 677.

404 Siehe oben Kapitel 3,A.

Wie auch in Deutschland herrscht in den Vereinigten Staaten jedoch ein hohes Misstrauen gegenüber staatlichen Tätigkeiten. Das Unwohlsein wird insbesondere verstärkt durch die mehr und mehr bekannt werdenden Überwachungstätigkeiten der US-Geheimdienste. Verschafft sich der Staat in dem derzeit angenommenen Ausmaß Zugriff auf private Datensammlungen, erschüttert dies nicht nur das Vertrauen der US-Bürger in den Staat. Mittelfristig erscheint es konsequent, dass dadurch die Bereitschaft der Bürger leidet, Daten gegenüber Privaten preiszugeben. Während bis dato vor allem der Staat als Bedrohung für die verfassungsmäßigen Rechte der Bürger wahrgenommen wird, wird sich diese Perzeption der Bevölkerung zweifelsohne ändern, wenn allgemein bekannt ist, dass der Staat in großem Maße Zugriff auf die gegenüber Privaten preisgegebenen Daten nimmt. Dann wird auch die Preisgabe gegenüber Privaten als Gefahr empfunden und vielleicht entsprechend reduziert werden. Gerade in dem verfassungsrechtlichen und gesellschaftlichen Kontext der USA erscheint es daher sinnvoll, von staatlicher Seite noch stärker als bis jetzt die Grenzen zu respektieren, die die Bürger dadurch setzen, dass sie Daten lediglich Dritten, nicht aber dem Staat anvertrauen.

Angesichts des öffentlichen Unmuts über Privatheitsverletzungen durch den Staat werden entsprechend erste Schritte eingeleitet, um die geheimdienstlichen Ausforschungen einzudämmen.[405] Diese Limitierung der Tätigkeiten von US-Geheimdiensten ist auch aus deutscher Sicht begrüßenswert, da sie unter Umständen auch zu reduzierter Überwachung deutscher Bürger oder Unternehmen durch US-Geheimdienste führen oder jedenfalls als Vorbild für eine Verringerung der Aktivitäten deutscher Geheimdienste dienen kann.[406]

Auch wenn es zur Erreichung eines globalen höheren Privatheitsschutzes wünschenswert wäre,[407] dass sich das US-Schutzniveau dem deutschen anpasste, ist davon nicht auszugehen. Jedoch könnte jedenfalls im Verhältnis Staat – Bürger der Schutz in den Vereinigten Staaten gestärkt werden, beispielsweise durch Abkehr von der umstrittenen Third-Party-Doktrin. Eine solche Entwicklung erscheint realistisch und wäre sachgerecht.

Anders stellt sich die Situation hinsichtlich der verfassungsrechtlichen Absicherung der Informationsfreiheit dar: Beide Verfassungen messen dieser an sich hohe Bedeutung zu. In Deutschland muss jedoch regelmäßig eine gleichberechtigte Balance zwischen der Informationsfreiheit und anderen betroffenen Gütern gefunden werden, in den USA fällt die Abwägung fast immer zugunsten der Informations-

---

405 So der jüngst erlassene USA Freedom Act, HR 2048, https://www.congress.gov/114/bills/hr2048/BILLS-114hr2048enr.pdf.

406 Weitgehend ungeklärt ist, in welchem Umfang der deutsche Staat direkt an der Arbeit der US-Geheimdienste beteiligt ist: *Fuchs/Goetz*, Geheimer Krieg, 2013, 139 ff.

407 Der Umstand, dass die Balance zwischen Privatheit und Sicherheit in den USA häufig zu Lasten der Privatheit ausfällt, beeinflusst den globalen Privatheitsschutz auf vielfältige Art, vgl. zum Einfluss der US-Vorgaben auf das Sammeln von Flugzeugpassagierdaten: *Baumann*, Grenzüberschreitender Datenaustausch, in: Dix/Franßen/Kloepfer u. a. (Hrsg.), Informationsfreiheit und Informationsrecht, 2015, 29 ff.

freiheit aus. Grund dafür ist die herausragende Stellung, die dem freien Fluss von Informationen im US-Rechtssystem zukommt.[408] Damit ist der Schutzgehalt der US-amerikanischen Informationsfreiheit als deutlich höher einzustufen als der der deutschen.

2. Allgemeinwohlbelange

Die durch die tatsächlichen Gefahren für Allgemeinwohlbelange tangierten Rechtsgüter finden in beiden Verfassungen Schutz.

Während der Privatheitsschutz in den USA hinsichtlich der informationellen Privatheit der Preisgebenden quasi nicht-existent ist, besteht durchaus ein Schutz, wenn die informationelle Privatheit Dritter bedroht wird. Jedoch treten auch die Privatheitsinteressen Dritter regelmäßig hinter der Redefreiheit (Erster Zusatzartikel) der Preisgebenden zurück, sobald es zu einer Abwägung kommt. Insofern besteht in den Vereinigten Staaten zwar ein Schutz der informationellen Privatheit Dritter, jedoch bei Weitem nicht auf dem deutschen Niveau. Dies zeigt sich auf einfachgesetzlicher Ebene sehr deutlich daran, dass sowohl nach Art. 7 DSRL als auch nach deutschem Recht (§ 4 Abs. 1 BDSG und § 12 Abs. 1 TMG) ein Vorfeldschutz besteht, da das sogenannte Verbotsprinzip Privaten grundsätzlich die Verarbeitung personenbezogener Daten untersagt und hierfür eine gesetzliche Grundlage oder Einwilligung verlangt. Zudem lässt die ausgereifte Judikatur zum Recht auf informationelle Selbstbestimmung in Deutschland einen höheren Schutzgrad der informationellen Privatheit Dritter in Deutschland annehmen als nach der sich noch in Entwicklung befindlichen US-Rechtslage.

Hinsichtlich der gesellschaftlichen Belange zeigt sich hingegen ein Gleichlauf, beide Rechtssysteme schreiben ihnen hohe Bedeutung zu. Angesichts des Bezugs gesellschaftlicher Aspekte zu der, gerade in den USA sehr starken, Meinungsfreiheit, könnte diesen in den Vereinigten Staaten jedoch in Zukunft ein erhebliches Gewicht in der dogmatischen Entwicklung des Privatheitsschutzes zukommen, während diese Schutzzwecke im deutschen Recht wohl sekundär bleiben werden.

[408] Zur Bedeutung des Ersten Zusatzartikels im US-Verfassungssystem sei auf die umfangreichen Vorabreiten anderer Autoren verwiesen: *Buchner*, Informationelle Selbstbestimmung im Privatrecht, 2006, 20 ff., 83 ff.; *Post*, Yellow Press and Privacy, GRUR Int 2006, 283, 292; *Whitman*, The Two Western Cultures of Privacy, 113 Yale L. J. (2004), 1151, 1209 und *Wittern*, Das Verhältnis von Right of Privacy und Persönlichkeitsrecht zur Freiheit der Massenmedien, 2004, 270 ff.

Kapitel 4

Mögliche Maßnahmen zur Verhinderung der Preisgabe

Kommt der Staat nach Abwägung der Chancen und Gefahren konkreter informationeller Preisgabe zu dem Ergebnis, dass die Gefahren für ein verfassungsrechtlich geschütztes Rechtsgut schwerwiegender sind als die Chancen für Einzelne oder das Gemeinwohl, kann er ein Bedürfnis nach Verhinderung der informationellen Preisgabe sehen. Das Recht kann dann – vorbehaltlich der verfassungsrechtlichen Zulässigkeit der Maßnahmen[1] – mit der informationellen Preisgabe der Internetnutzer auf zwei grundsätzlich unterschiedliche Weisen umgehen: Indem es die negativen Folgen informationeller Preisgabe nachträglich abmildert oder die Preisgabe bereits von Beginn an verhindert.

Die Abmilderung der negativen Folgen erfolgt in Deutschland ex post durch zahlreiche einfachgesetzliche Datenschutzbestimmungen, die beispielsweise die Modalitäten der automatisierten Datenverarbeitung regeln,[2] Datensicherheit gewährleisten sollen oder den Nutzern Auskunfts-, Löschungs- oder Berichtigungsrechte geben.[3] Während diese Vorgaben in Deutschland sektorenübergreifend für jeden Umgang mit personenbezogenen Daten gelten, bestehen in den Vereinigten Staaten sektorspezifische Regelungen, die weit weniger Bereiche erfassen als ihre deutschen Pendants.[4]

Die vorliegende Arbeit beschränkt sich auf Konzepte zur Verhinderung der informationellen Preisgabe ex ante und lässt all jene Schritte außer Acht, die nach Datenpreisgabe durch die Nutzer erfolgen. Während die vorgenannten Detailregelungen vielfach untersucht sind, ist die Frage nach der Verhinderung bislang nicht oder nur eingeschränkt behandelt worden. Wegen des Problems eines – figurativen – Zurückholens von Daten stellt die Verhinderung der Preisgabe die ungleich effektivere Maßnahme dar. Es stellt sich deshalb die Frage, ob diese zulässig ist.

Angesichts allgemeingültiger Wirkungsweisen der Maßnahmen und vergleichbarer gesellschaftlicher Ausgangslagen kann informationelle Preisgabe sowohl in

---

[1] Dieses Kapitel beschränkt sich auf die Darstellung der tatsächlich möglichen Mittel zur Verhinderung informationeller Preisgabe. Die rechtliche Gebotenheit beziehungsweise Zulässigkeit der Maßnahmen ist Gegenstand der Kapitel 5 und 6.

[2] Dies kann geschehen etwa durch die Bindung an definierte Verarbeitungszwecke und die Beschränkung auf die zu diesen Zwecken erforderliche Datenverarbeitung.

[3] Einen Überblick möglicher Rechte bieten: *Roßnagel/Pfitzmann/Garstka*, Modernisierung des Datenschutzrechts, DuD 2001, 253, 261 f. und *Weidner-Braun*, Der Schutz der Privatsphäre und des Rechts auf informationelle Selbstbestimmung, 2012, 137 ff.

[4] Einen Überblick bietet: *Genz*, Datenschutz in Europa und den USA, 2004, 50 ff.

Deutschland als auch in den Vereinigten Staaten faktisch durch identische Mittel verhindert werden. Eine Differenzierung nach Ländern ist deshalb nicht erforderlich.

Die möglichen Maßnahmen zur Verhinderung informationeller Preisgabe können in verschiedene Kategorien gefasst werden. *Calo* unterteilt in „code", „nudge" und „notice" beziehungsweise in „friction" und „facilitation".[5] Er führt aus: „Friction refers to creating barriers – physical or otherwise – to the conduct citizens would otherwise carry out. Facilitation refers to helping citizens develop and consummate their intentions."[6] Gleichzeitig weist er jedoch darauf hin, dass die Übergänge zwischen den verschiedenen Formen im Einzelfall verschwimmen können. Weiter unterscheidet *Zuiderveen Borgesius* „empowering", „protection" und „nudges".[7] *van Aaken* schließlich unterteilt in „Wahlverbote" und „Wahlhilfen".[8]

Im Rahmen der vorliegenden Analyse werden die drei Kategorien erzwungener Schutz (siehe A), Unterstützung informationellen Selbstschutzes (siehe B) und Schutz durch Entscheidungsarchitekturen gewählt (siehe C). Auch wenn die Grenzen im Einzelfall verschwimmen können, bietet diese Unterteilung eine sinnvolle Grobstruktur für die nachfolgende verfassungsrechtliche Analyse.[9] Während sich Maßnahmen zur Verhinderung informationeller Preisgabe traditionellerweise auf erzwungenen Schutz und die Unterstützung informationellen Selbstschutzes konzentrieren, findet derzeit gerade in den Vereinigten Staaten eine hitzige Diskussion über den ergänzenden oder alternativen Einsatz von Entscheidungsarchitekturen statt.

A. Erzwungener Schutz

Die erste Möglichkeit zur Verhinderung informationeller Preisgabe lässt sich als erzwungener Schutz oder auch als „Wahlverbot"[10] charakterisieren. Der Staat entscheidet generalisierend, welche Formen der Preisgabe mehr Risiken als Chancen mit sich bringen und sucht sie zu verhindern, indem er verbindliche Regeln über die Preisgabe aufstellt.

Die Verhinderung informationeller Preisgabe kann geschehen durch Verbote (siehe I) und/oder durch die Verpflichtung zur Technikgestaltung in einer Weise, die Preisgabe unmöglich macht (siehe II).

---

[5] *Calo*, Code, Nudge, or Notice?, 4.2013, 1 ff.

[6] *Calo*, Code, Nudge, or Notice?, 4.2013, 4.

[7] *Zuiderveen Borgesius*, Consent to Behavioural Targeting in European Law, 7.2013, 46 ff.

[8] *Van Aaken*, Begrenzte Rationalität und Paternalismusgefahr, in: Anderheiden/Bürkli/Heinig u. a. (Hrsg.), Paternalismus und Recht, 2006, 109, 124 ff.

[9] Siehe unten Kapitel 5 und Kapitel 6.

[10] *Van Aaken*, Begrenzte Rationalität und Paternalismusgefahr, in: Anderheiden/Bürkli/Heinig u. a. (Hrsg.), Paternalismus und Recht, 2006, 109, 124.

Erzwungener Schutz kann als Verbot oder Verpflichtung gegenüber den Nutzern oder den verantwortlichen Stellen umgesetzt werden. Eine verantwortliche Stelle ist dabei entsprechend der Definition in § 3 Abs. 7 BDSG jede Person oder Stelle, die personenbezogene Daten für sich selbst erhebt, verarbeitet oder nutzt oder dies durch Andere im Auftrag vornehmen lässt.[11] Ein Verbot oder die technische Unmöglichmachung der Preisgabe gegenüber den Nutzern führen im Ergebnis dazu, dass die verantwortlichen Stellen die personenbezogenen Daten nicht erheben, verarbeiten und nutzen dürfen oder können; ein Verbot der Erhebung oder ihre technische Unmöglichmachung dazu, dass die Nutzer die personenbezogenen Daten nicht preisgeben dürfen oder können.

In beiden Fällen werden die Interessen sowohl der Nutzer als auch der verantwortlichen Stellen betroffen. Die Annahme, indirekter Paternalismus in Form von gegen die verantwortlichen Stellen gerichteten Maßnahmen berühre die Belange der Nutzer nicht, geht fehl.[12] Teilweise wird demgemäß unterteilt in puren Paternalismus, bei dem die Freiheit derjenigen beschnitten wird, die geschützt werden sollen und „unpuren" Paternalismus, bei dem in die Freiheit Anderer eingegriffen wird, um die Betroffenen zu schützen.[13] Wird der Schutz vorverlagert, indem der Staat auf Dritte einwirkt und so die Selbstschädigung abwendet, ist dies auch an den Grundrechten der Selbstschädiger zu messen.[14] Praktisch ist es für die Nutzer nur bedingt relevant, gegen wen sich die Maßnahme richtet, wenn sie im Ergebnis von der Preisgabe und damit von der Grundrechtsausübung abgehalten werden.

I. Verhinderung durch Verbot

Direkter Ansatzpunkt ist es, den Nutzern oder den verantwortlichen Stellen bestimmte Verhaltensweisen zu untersagen. Im Folgenden sollen sowohl abstrakte als auch konkrete Maßnahmen der Verhinderung durch Verbot dargestellt werden.

Beispielsweise kann Minderjährigen die Nutzung sozialer Netzwerke verboten wird. Weiter kann es untersagt werden, bestimmte Daten wie genetische Daten, Informationen über Erbkrankheiten, Ergebnisse von Lügendetektortests oder Mitschnitte eigener sexueller Handlungen preiszugeben. Durch den Erlass derartiger Regelungen werden die Preisgebenden zum Unterlassen der Preisgabe gezwungen.

---

[11] Im Rahmen dieser Untersuchung nicht relevant ist die Frage, ob es entsprechend dem Verständnis von Art. 2 lit. d DSRL auch mehrere, parallele verantwortliche Stellen geben kann.

[12] So aber *Weber* im Kontext des Dopings: *Weber*, in: ders. (Hrsg.), Betäubungsmittelgesetz, 2013, § 6a AMG, Rn. 6.

[13] *Dworkin*, Paternalism, in: Sartorius (Hrsg.), Paternalism, 1983, 19, 22.

[14] *Fateh-Moghadam*, Die Einwilligung in die Lebendorganspende, 2008, 79; *Fischer*, Die Zulässigkeit aufgedrängten staatlichen Schutzes vor Selbstschädigung, 1997, 105 f.; vgl.: *Schroth*, Die Begrenzung des Spenderkreises im Transplantationsgesetz als Problem der paternalistischen Einschränkung menschlicher Freiheit, in: Schünemann/Müller/Philipps (Hrsg.), Das Menschenbild im weltweiten Wandel der Grundrechte, 2002, 35, 40.

Weiter kann Preisgabe dadurch verhindert werden, dass Nutzer bestimmte Einwilligungen nicht erteilen dürfen, selbst wenn sie wollen.[15] Das Einwilligungsverbot kann sich dabei sowohl auf die Datenerhebung als auch auf bestimmte Verwendungen beziehen. So gestattet beispielsweise Art. 9 EU-DS-GVO-E den EU-Mitgliedstaaten, eine Einwilligung in die Verarbeitung besonders sensibler personenbezogener Daten zu untersagen. Erfasst sind Daten, die Aufschluss geben über „Rasse“, ethnische Herkunft, politische Überzeugungen, Religions- oder Glaubenszugehörigkeit, Zugehörigkeit zu einer Gewerkschaft sowie genetische Daten, Daten über die Gesundheit oder das Sexualleben, ferner Daten über Strafurteile oder damit zusammenhängende Sicherungsmaßregeln. Ein in Deutschland nicht[16] umgesetzter Vorläufer dieser Regelung befindet sich bereits in Art. 8 Abs. 2 lit. a DSRL. Auch kann beispielsweise festgelegt werden, dass Browser Nutzer bis zu einem bestimmten Grad selbst dann nicht tracken dürfen, wenn die Nutzer einwilligen. Ebenso zu denken ist an absolute Verknüpfungsverbote, die Nutzer auch durch ihre informierte, freiwillige und selbstbestimmte Einwilligung nicht aufheben können.

II. Verhinderung durch Technikgestaltung

Weiter kann die Preisgabe technisch unmöglich gemacht werden. Während ein Verbot unerwünschtes Verhalten nicht unterbindet, sondern mit nachträglich wirkenden Sanktionen belegt, setzen technische Verhinderungsmaßnahmen schon vor der Preisgabe an. Diese Mechanismen sollen im Folgenden abstrakt dargestellt werden:

Nach *Lessig* erfolgt die Regulierung des Cyberspace durch Code, also durch die Architektur des Cyberspace.[17] Es wirken vier auf die zu Regulierenden einwirkende Zwänge zusammen: Gesetz, soziale Normen, Märkte und Code.[18] Der Gesetzgeber kann durch Gesetz direkten Zwang ausüben oder auf die anderen Zwänge Einfluss nehmen, beispielsweise durch Bildungsgesetze auf soziale Normen, durch Steuern auf die Märkte und durch die in diesem Absatz beschriebenen Gesetze, die bestimmte Technikgestaltung vorschreiben, auf Code. Code ist selbst ausführend und wirkt, einmal implementiert, ununterbrochen bis zu seiner Abschaffung.[19]

---

[15] Weitreichend ist die Forderung *Radlanskis*, der fordert, datenschutzrechtliche Einwilligungen in Zukunft nur noch dann zuzulassen, wenn der legitimierte Datenumgang im objektiven Interesse der Preisgebenden liegt, *Radlanski*, Das Konzept der Einwilligung in der datenschutzrechtlichen Realität, 2015 (im Erscheinen).

[16] In Deutschland regelt § 4a Abs. 3 BDSG lediglich eine Verschärfung der Anforderungen an die Einwilligung, die sich bei Angaben über die rassische und ethnische Herkunft, politische Meinungen, religiöse oder philosophische Überzeugungen, Gewerkschaftszugehörigkeit, Gesundheit oder Sexualleben ausdrücklich auf diese erstrecken muss.

[17] Siehe zu den folgenden Ausführungen, soweit nicht anders angegeben: *Lessig*, Code, 2006, 5 ff.

[18] *Lessig*, Code, 2006, 132, 124 ff.; kritisch: *Rotenberg*, Fair Information Practices and the Architecture of Privacy, 1 Stanford Tech. L. Rev. (2001), 1 ff.

[19] *Lessig*, Code, 2006, 342 f.

Während *Lessig* davon ausgeht, dass Angebot und Nachfrage regelmäßig bestimmen, welcher Code sich durchsetzt, fordern andere Stimmen richtigerweise, dass der Staat lenkend eingreift.[20] Der Staat kann demnach auf den Code Einfluss nehmen, indem er durchzusetzende Ziele bestimmt und die – im übertragenen Sinn – Architekten zu entsprechenden Gestaltungen bewegt. Dies kann er durch Verpflichtungen erreichen, aber auch durch das Setzen von Anreizen, beispielsweise durch Gewährung von Subventionen bei Einführung der gewünschten technischen Änderungen.[21]

So, wie in der Offline-Welt Türen am Betreten des Hauses hindern und Speedbumps zur Reduzierung der Geschwindigkeit von Fahrzeugen zwingen, könnten auch technische Vorrichtungen informationelle Preisgabe verhindern. Zu denken ist beispielsweise an den Einsatz von Textanalysesoftware, die beleidigende Äußerungen erkennt und die Veröffentlichung entsprechender Posts in sozialen Netzwerken blockt. Entsprechend könnten durch Bildanalyseprogramme auch sexuell verfängliche Bilder erkannt und ihr Hochladen verhindert werden.

Abzugrenzen ist die verbindliche Verhinderung durch Technikgestaltung von der Möglichkeit der Nutzer, freiwillig von Mitteln zum technischen Selbstschutz[22] Gebrauch zu machen. Letztere sind einschlägig, wenn die Preisgabe nicht unabhängig vom Willen der Nutzer verhindert, sondern ihnen lediglich eine selbstbestimmte Wahl darüber ermöglicht wird, ob sie durch technische Schritte ihre Preisgabe limitieren wollen. Wird Datenschutz durch Technik den Nutzern jedoch aufoktroyiert, stellt dies eine technische Verhinderung der Preisgabe dar.

B. Unterstützung informationellen Selbstschutzes

Anstatt den Nutzern bestimmte staatliche Wertungen durch Verbote oder technische Maßnahmen aufzuzwingen, kann ihnen informationeller Selbstschutz ermöglicht werden. Dadurch können sie eine individuelle Kosten-Nutzen-Analyse durchführen, in die sie die für sie relevanten Aspekte einstellen. Auf dieser Basis können sie dann in eigener Verantwortung entscheiden. Die Rede ist treffend von einem „privacy self-management“.[23]

Der Staat kann informationellen Selbstschutz unterstützen, indem er entsprechende Infrastrukturleistungen zur Verfügung stellt, Anreiz zu ihrer Entwicklung setzt und beispielsweise durch monetäre Unterstützung oder Vorrang bei Beschaffungen durch die öffentliche Hand fördert. So wird in Art. 23 Abs. 1a der LIBE-Fassung des Entwurfs der EU-Datenschutz-Grundverordnung vorgeschrieben, dass bei

---

[20] *Cohen*, DRM and Privacy, 18 Berkeley Tech. L. J. (2003), 575, 609.

[21] *Lessig*, Code, 2006, 66 f.

[22] Siehe unten Kapitel 4,B.III.

[23] *Solove*, Privacy Self-Management and the Consent Dilemma, 126 Harvard L. Rev. (2013), 1880, 1882 ff.

der Vergabe öffentlicher Aufträge Voraussetzung ist, dass die Grundsätze von Datenschutz durch Technik durch die Auftragnehmer eingehalten werden.

Die rechtliche Absicherung der Nutzung informationeller Selbstschutzmöglichkeiten ist dabei zu gewährleisten. Beispielsweise wird vorgeschlagen, das Senden eines Do-not-track-Signals als Widerspruch gegen die Erstellung von Nutzerprofilen nach § 15 Abs. 3 Satz 1 TMG zu werten.[24] Weiter sollten die Mittel des informationellen Selbstschutzes jedenfalls nicht verboten und ihr Einsatz nicht zum Anlass genommen werden, Nutzer vonseiten der Ermittlungsbehörden als verdächtig einzustufen, wie es jedoch gelegentlich im Falle der Anwendung von Verschlüsselungstechnologien geschieht.[25]

Alle staatlichen Maßnahmen zur Unterstützung informationellen Selbstschutzes sind dadurch gekennzeichnet, dass der Staat der Entscheidung der Nutzer gegenüber neutral bleibt und nicht versucht, die Nutzer in Richtung Privatheitswahrung zu drängen. Damit ist den Mitteln gemein, dass die Verantwortung bei den Nutzern liegt.

Aus der Bandbreite an realiter möglichen Maßnahmen des informationellen Selbstschutzes sollen im Folgenden die wohl bedeutendsten Beispiele herausgegriffen werden: die konventionelle Unterrichtung (siehe I), alternative Unterrichtungsmethoden (siehe II), technische Selbstschutzmöglichkeiten (siehe III) und Datenschutz als Bildungsauftrag (siehe IV).

I. Konventionelle Unterrichtung

Zunächst können die verantwortlichen Stellen verpflichtet werden, die Nutzer über alle mit der Datenerhebung im Zusammenhang stehenden Fakten zu informieren. Die klassische Unterrichtung durch Worte stellt damit die Basis des Maßnahmenkatalogs zur Unterstützung informationellen Selbstschutzes dar. Als Beispiele zu nennen sind § 4a Abs. 1 Satz 2 BDSG[26] und im Internet vor allem § 13 TMG[27].

Ihr kommt nach dem bisherigen deutschen Regelungskonzept die tragendste Rolle zu. Auch in den Vereinigten Staaten stellen die, von den verantwortlichen Stellen häufig freiwillig ausgegebenen, Datenschutzrichtlinien die Grundlage für die mit der Preisgabe zusammenhängenden Entscheidungen der Bürger dar.

[24] *Berliner Beauftragter für Datenschutz und Informationsfreiheit*, Bericht 2011, 2011, 169. Da die Funktion jedoch auch ohne Kenntnis der Nutzer als Voreinstellung im Browser aktiviert sein kann, scheint die Einordnung als Widerspruch nach geltendem Recht fragwürdig.

[25] *Schaar*, Lässt sich die globale Internetüberwachung noch bändigen?, ZRP 2013, 214, 216.

[26] Dieser lautet: „[Der Betroffene] ist auf den vorgesehenen Zweck der Erhebung, Verarbeitung oder Nutzung sowie, soweit nach den Umständen des Einzelfalles erforderlich oder auf Verlangen, auf die Folgen der Verweigerung der Einwilligung hinzuweisen."

[27] Dessen Absatz 1 lautet: „Der Diensteanbieter hat den Nutzer zu Beginn des Nutzungsvorgangs über Art, Umfang und Zwecke der Erhebung und Verwendung personenbezogener Daten sowie über die Verarbeitung seiner Daten in Staaten außerhalb des Anwendungsbereichs der [DSRL] in allgemein verständlicher Form zu unterrichten, sofern eine solche Unterrichtung nicht bereits erfolgt ist."

Um jedoch auf eine häufig vorhandene Überforderung der Nutzer zu reagieren, werden weitere Maßnahmen zur Unterstützung informationellen Selbstschutzes diskutiert.

II. Alternative Unterrichtungsmethoden

In Ergänzung zur Unterrichtung durch Worte können Anwendungen in einer Weise gestaltet werden, aus der die Nutzer erkennen, welche Daten erhoben werden und bei der sie hierauf in einfacher Weise Einfluss nehmen können. Beispielsweise können Wahlmöglichkeiten in Datenschutzeinstellungen in sozialen Netzwerken einheitlich und intuitiv dargestellt werden. Auch können Symbolsysteme verwendet werden, die Aufschluss über die durch die Anbieter und Dritte erfolgende automatisierte Datenverarbeitung geben. Beispiel ist das Mozilla Privacy Icons Project.[28] Auch die LIBE-Fassung des Entwurfs der EU-Datenschutz-Grundverordnung enthält in Anhang 1 (zu Art. 13a) eine Liste solcher, jedoch nicht unbedingt intuitiv verständlicher, Symbole.

Weiter können Verfahren eingeführt werden, die die Nutzer nicht nur allgemein über mögliche Datenerhebungen und -verwendungen aufklären, sondern ihnen die konkreten persönlichen Konsequenzen zeigen.[29] Solche Unterrichtungsmethoden sind Teil des vorgeschlagenen Konzepts der „visceral notice“.[30] Wörtlich übersetzt sollen die Nutzer die Privatheitsunterrichtung in ihren Eingeweiden spüren. Gemeint ist der Terminus freilich im übertragenen Sinn. Als Offline-Beispiel dienen imitierte Motorengeräusche, die Elektroautomobile produzieren, um Fußgänger auf das Herannahen eines an sich geräuschlosen Elektroautomobils hinzuweisen. Die Privatheitsunterrichtung soll demnach nicht auf einen kognitiven Erfassungsprozess angewiesen sein, sondern direkt die Erfahrung verändern, die die Nutzer mit dem Produkt machen („notice as experience“).[31]

Das Google Dashboard beispielsweise gibt den Nutzern teilweise Auskunft darüber, welche verschiedenen Daten Google im Laufe der Jahre im Rahmen der Nutzung verschiedener Services und verschiedener Endgeräte über die Nutzer gesammelt hat.[32] Die Nutzer können dann, jedenfalls oberflächlich, Daten löschen und in Zukunft bewusstere Preisgabe praktizieren. Der Yahoo Ad Interest Manager zeigt den Nutzern partiell, welche Annahmen Yahoo über sie durch Datenanalyse gewonnen hat und gibt ihnen die Möglichkeit, diese Annahmen teilweise zu korrigieren.[33]

---

[28] https://wiki.mozilla.org/Privacy_Icons; *Kelbert/meh Shirazi/Simo u. a.*, State of Online Privacy, in: Buchmann (Hrsg.), Internet Privacy, 2012, 189, 247.

[29] *Calo*, Against Notice Skepticism in Privacy (and Elsewhere), 87 Notre Dame L. Rev. (2012), 1027, 1043.

[30] *Calo*, Against Notice Skepticism in Privacy (and Elsewhere), 87 Notre Dame L. Rev. (2012), 1027, 1036.

[31] *Calo*, Against Notice Skepticism in Privacy (and Elsewhere), 87 Notre Dame L. Rev. (2012), 1027, 1033 f.

[32] https://www.google.com/dashboard.

[33] https://info.yahoo.com/privacy/us/yahoo/opt_out/targeting/.

Das Facebook View-As-Tool ermöglicht es den Nutzern zu prüfen, wie ihre Profile für bestimmte andere Nutzer oder die Öffentlichkeit aussehen.[34] Derartige Mittel erlauben den Nutzern informiertere Entscheidungen über ihre künftige informationelle Preisgabe.

III. Technischer Selbstschutz

Ein weiteres Instrument zur Unterstützung informationellen Selbstschutzes ist das Konzept des technischen Selbstschutzes. Unter den Schlagwörtern Datenschutz durch Technik, Privacy by Design, Privacy Enhancing Technologies et cetera werden Mittel diskutiert, die auf die Schaffung von technischen Rahmenbedingungen zielen, in denen die Preisgabe nicht zu nicht erforderlicher und im Regelfall nicht bewusster Datenerhebung und -verarbeitung führt.[35] Dadurch werden den Nutzern selbstbestimmte Entscheidungen über die informationelle Preisgabe ermöglicht, da unbewusste Preisgabe verhindert wird. Datenschutz durch Technik integriert Datenschutz in Dienste und Verfahren.[36] Der Schwerpunkt liegt auf der Datenvermeidung und -sparsamkeit (vgl. § 3a BDSG). Unter Datensparsamkeit versteht man eine System- und Verfahrensgestaltung, die gemäß dem Erforderlichkeitsprinzip das Anfallen personenbezogener Daten minimiert und die Verwendungsmöglichkeiten einschränkt, um die Zweckbindung zu garantieren.[37] Datensparsamkeit bedeutet, informationstechnische Systeme derart zu gestalten, dass so wenig personenbezogene Daten wie möglich so kurz wie möglich anfallen.[38]

Die vorliegende Arbeit konzentriert sich dabei auf diejenigen Mittel, die vor und bei der Preisgabe ansetzen und lässt ausschließlich nachträglich wirkende Mittel außer Acht.

Zu denken ist zunächst an die Schaffung anonymer beziehungsweise jedenfalls pseudonymer Strukturen.[39] Anonyme Datenerhebung lässt Personenbezug erst gar nicht entstehen: Die Wahrscheinlichkeit der erneuten Zuordnung der Daten ist so

[34] https://www.facebook.com/help/288066747875915.

[35] Beispielsweise schreibt Art. 23 Abs. 1 EU-DS-GVO-E die Umsetzung von Datenschutz durch Technik vor; zur Umsetzung von technischem Selbstschutz in der EU-Datenschutzreform und möglichen Regulierungsansätzen, siehe: *Hornung*, Regulating privacy enhancing technologies, 26 Innovation: The European Journal of Social Sciences (2013), 181 ff.; siehe aktuell auch den ENISA-Report: *Danezis/Domingo-Ferrer/Hansen u. a.*, Privacy and Data Protection by Design, 12.2014.

[36] *Federath/Pfitzmann*, Technische Grundlagen, in: Roßnagel (Hrsg.), Handbuch Datenschutzrecht, 2003, 61, 63 ff., Rn. 5 ff. und *Roßnagel/Pfitzmann/Garstka*, Modernisierung des Datenschutzrechts, 2001, 36.

[37] *Hansen*, Privacy Enhancing Technologies, in: Roßnagel (Hrsg.), Handbuch Datenschutzrecht, 2003, 291, 305, Rn. 47.

[38] *Hansen*, Privacy Enhancing Technologies, in: Roßnagel (Hrsg.), Handbuch Datenschutzrecht, 2003, 291, 305, Rn. 48.

[39] Grundlegend: *Roßnagel/Scholz*, Datenschutz durch Anonymität und Pseudonymität, MMR 2000, 721 ff.; *Roßnagel/Pfitzmann/Garstka*, Modernisierung des Datenschutzrechts, 2001, 148 ff.; zum Zusammenhang zwischen Anonymität und Ehrschutz im Internet: *Heckmann*, Persönlichkeitsschutz im Internet, NJW 2012, 2631 ff.

gering, dass sie nach Lebenserfahrung oder Stand der Wissenschaft praktisch ausscheidet.[40] Auch pseudonyme Daten stellen für alle diejenigen, die keine Kenntnis über die Zuordnungsregel haben, keine personenbezogenen Daten dar, da die Nutzer Kennzeichen benutzen, durch die die Wahrscheinlichkeit, dass Daten ihnen zugeordnet werden können, so gering ist, dass sie ohne Kenntnis dieser Regel nach der Lebenserfahrung oder dem Stand der Wissenschaft praktisch ausscheidet.[41] Anonymisierung und Pseudonymisierung können an verschiedenen Stellen ansetzen. So können beispielsweise durch die Nutzung von The Onion Routing (TOR) Verbindungsdaten anonymisiert werden.[42] Die Schaffung anonymer und pseudonymer Strukturen kann ergänzend einhergehen mit der Möglichkeit zum Identitätsmanagement, also der Verwaltung und Pflege digitaler Identitäten.[43]

Zudem können mithilfe von Verschlüsselungstechnologien Daten übertragen werden, ohne dass beispielsweise Intermediäre auf die Daten im Klartext Zugriff haben. Der E-Mail-Verschlüsselungsstandard OpenPGP ermöglicht den Versand verschlüsselter und signierter E-Mails,[44] der Cloud-Anbieter Tresorit das verschlüsselte Speichern von Daten in der Cloud.[45]

Ein weiteres Beispiel ist die Einführung und Durchsetzung eines einheitlichen Do-not-track-Regimes, welches den Nutzern eine einfache und wirksame Entscheidung darüber ermöglicht, ob und inwieweit ihr Nutzungsverhalten durch Dritte verfolgt werden darf. Trotz breiten Konsenses hinsichtlich der grundsätzlichen Nützlichkeit solcher Systeme gestaltet sich die federführend vom World Wide Web Consortium übernommene Ausarbeitung jedoch schwierig.[46] Das Unabhängige Landeszentrum für Datenschutz Schleswig-Holstein kritisiert daher nicht zu Unrecht: „Der ursprünglich vielversprechende Ansatz von ‚Do Not Track' ist […] so weit verwässert, dass der Name der Initiative eher als Verbrauchertäuschung eingestuft werden muss: Unter dem Mantel von ‚Do Not Track' wollen Werbefirmen ihr rechtswidriges Verhalten legitimieren und die Nutzenden in falscher Sicherheit wiegen."[47] Trotz Unklarheiten im Detail haben die führenden Internetbrowser, unter anderem Mozilla Firefox, Microsoft Internet Explorer und Google Chrome, Do-not-track-Optionen in ihr Angebot integriert.[48]

---

[40] *Roßnagel*, Konzepte des Selbstdatenschutzes, in: ders. (Hrsg.), Handbuch Datenschutzrecht, 2003, 325, 345, Rn. 57. In der Literatur wird teilweise zwischen der absoluten und der, hier beschriebenen, relativen Anonymisierung unterschieden.

[41] *Roßnagel*, Konzepte des Selbstdatenschutzes, in: ders. (Hrsg.), Handbuch Datenschutzrecht, 2003, 325, 346 f., Rn. 60.

[42] https://www.torproject.org/.

[43] *Roßnagel/Pfitzmann/Garstka*, Modernisierung des Datenschutzrechts, DuD 2001, 253, 260.

[44] http://www.openpgp.org/.

[45] https://tresorit.com/.

[46] http://www.w3.org/2011/tracking-protection/.

[47] *Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein*, Selbstregulierung bei „Do Not Track" gescheitert, 19.10.2012.

[48] https://www.mozilla.org/en-US/dnt/; http://windows.microsoft.com/de-DE/internet-explorer/use-tracking-protection#ie=ie-10; https://support.google.com/chrome/answer/114836.

Generell können Optionen geschaffen werden, die den Nutzern den Gebrauch von Web-Browsern in einer Weise ermöglichen, in der sie selbstbestimmt über ihre Datenpreisgabe entscheiden können. Dies kann geschehen durch die Integration technischer Selbstschutzmöglichkeiten in die Browser oder durch Bereitstellung entsprechender Add-ons, die beispielsweise bestimmte Skripte oder Cookies blockieren können.[49] Einen ähnlichen Ansatz verfolgt das Platform for Privacy Preferences Project (P3P) des World Wide Web Consortiums. P3P-Agenten in den Browsern der Nutzer vergleichen deren Datenschutzpräferenzen mit der maschinenlesbaren P3P-Datenschutzerklärung der angefragten Webseiten und informieren die Nutzer über Abweichungen, sodass ihnen auf dieser Basis eine Entscheidung über die Aufgabe ihrer Privatheit ermöglicht wird.[50] Auch werden textbasierte Programme wie Privee entwickelt, die den Wortlaut von Datenschutzerklärungen auslesen und auswerten können, um den Nutzern darzustellen, wie privatheitsfreundlich die Datenschutzbestimmungen einer Webseite sind.[51]

Weiter können Proxy-Server als Schnittstelle zwischen Nutzern und Browsern dienen, damit aller Internet-Traffic entsprechend den Proxy-Einstellungen behandelt wird. So können Personally Identifiying Protocol Headers aussortiert, das Lesen oder Setzen von Cookies verhindert oder JavaScript Code blockiert werden.[52]

Beispiel für eine zeitliche Begrenzung der Preisgabe ist das diskutierte Verfallsdatum von Daten, das in nicht ganz zutreffender Weise auch gleichgesetzt wird mit einem „digitalen Radiergummi“.[53] In diese Richtung geht auch das Pilotprojekt des sozialen Netzwerks Facebook, das es Nutzern ermöglicht, ihre Posts mit einem Ablaufdatum zu versehen.[54] Dabei ist jedoch wohl davon auszugehen, dass die Einträge nach diesem Zeitpunkt nicht vollständig gelöscht werden, sondern lediglich nicht mehr sichtbar sind.

---

[49] Praktische Beispiele: siehe: *Kelbert/meh Shirazi/Simo u.a.*, State of Online Privacy, in: Buchmann (Hrsg.), Internet Privacy, 2012, 189, 249.

[50] http://www.w3.org/P3P/.

[51] *Zimmeck/Bellovin*, Privee: An Architecture for Automatically Analyzing Web Privacy Policies, in: Proceedings of the 23rd USENIX Security Symposium, 2014, 1 ff.

[52] Praktische Beispiele, siehe: *Kelbert/meh Shirazi/Simo u.a.*, State of Online Privacy, in: Buchmann (Hrsg.), Internet Privacy, 2012, 189, 249 f.

[53] *Redaktion beck-aktuell*, De Maizière für „digitalen Radiergummi“ im Internet, becklink 23.6.2010, 1002049 ff. und *dies.*, Aigner schlägt Verfallsdatum für Internet-Dateien vor, becklink 10.1.2011, 1008988 ff. Diese Gleichsetzung geht partiell fehl. Während die Daten nach Ablauf ihres Verfallsdatums ohne Einwirkung der Preisgebenden verschwinden sollen, muss ein Radiergummi erst durch die Preisgebenden angewendet werden, um das Verschwinden der Daten herbeizuführen. Technisch ist die Idee des „digitalen Radiergummis“ jedenfalls dann vollständig gescheitert, wenn darunter ein effektives Radieren verstanden wird, siehe dazu auch: *Hornung/Hofmann*, Ein „Recht auf Vergessenwerden“?, JZ 2013, 163 ff. Den Versuch, eine technische Lösung zu erarbeiten, stellte unter anderem der Ideenwettbewerb des Bundesministeriums des Inneren dar, siehe: *Bundesministerium des Innern*, Ideenwettbewerb „Vergessen im Internet“, 7.5.2012.

[54] *Hamburger*, Facebook tests Snapchat-like expiration dates for your posts, 10.9.2014.

IV. Datenschutz als Bildungsauftrag

Schließlich werden als staatliche Mittel zur Verhinderung informationeller Preisgabe Maßnahmen vorgeschlagen, die unter den Schlagwörtern Datenschutz als Bildungsauftrag, Steigerung von Datenschutzkompetenz, Sensibilisierung und Befähigung et cetera diskutiert werden.[55] Durch Unterrichtung und Aufklärung sollen die Bürger in die Lage versetzt werden, selbstbestimmt über ihre informationelle Preisgabe zu entscheiden. Diese Befähigung kann durch die Erziehungsberechtigten, im Rahmen von Schul- und Hochschulbildung, aber auch durch Bildungsangebote beispielsweise an Volkshochschulen und durch Aufklärungskampagnen erfolgen. Hinzu kommt Unterrichtungsarbeit von Kammern und Verbänden. Als Beispiel dienen kann der, vom Europarat initiierte und jährlich am 28. Januar stattfindende, European Data Protection Day, an dem europaweit Veranstaltung zur Datenschutzaufklärung durchgeführt werden. Der Fantasie sind keine Grenzen gesetzt, wie auch das Spiel Data Dealer zeigt, in dem die Nutzer selbst zu Datensammlern werden.[56] Bei allen derartigen Maßnahmen ist auf eine alters- und schichtenspezifische Differenzierung der Bildungsangebote zu achten.[57]

Der Bildungsauftrag kann drei konventionelle Themengebiete umfassen: Zunächst kann über den Wert informationeller Privatheit und damit auch über die Gefahren informationeller Preisgabe für die Einzelnen und das Allgemeinwohl aufgeklärt werden. Hinzu treten kann eine Unterrichtung über die technischen Hintergründe der Datenerhebungen, -verarbeitungen und -nutzungen und über technische Selbstschutzmöglichkeiten. Schließlich kann aufgeklärt werden über rechtliche Selbstschutzmöglichkeiten, wie Auskunfts-, Widerrufs-, Löschungs- und Berichtigungsrechte, das für ihre Durchsetzung erforderliche Prozedere sowie Funktion und Anrufungsmöglichkeit der Datenschutzbeauftragten. Die letztgenannten Formen des rechtlichen Selbstschutzes setzen jedoch erst nach Preisgabe der Daten an und bleiben, abgesehen von der Aufklärung über sie, für die vorliegende Arbeit außer Betracht.

Darüber hinaus kann erwogen werden, die Nutzer auch über Anomalien im menschlichen Verhalten[58] aufzuklären und ihnen so einen bewussteren Umgang mit vorhersehbaren Irrationalitäten zu ermöglichen.[59]

---

[55] Europäische Strategie für ein besseres Internet für Kinder vom 2.5.2012, 9 ff.; dazu: *Europäischer Datenschutzbeauftragter*, Stellungnahme 17.7.2012, 5 ff.; *Gimmler*, Medienkompetenz und Datenschutzkompetenz in der Schule, DuD 2012, 110 ff.; *Grimmelmann*, Saving Facebook, 94 Iowa L. Rev. (2009), 1137, 1203 ff.; *Internet & Gesellschaft Co:llaboratory*, Gleichgewicht und Spannung zwischen digitaler Privatheit und Öffentlichkeit, 11.2011, 66 ff. und *Wagner*, Digitale Aufklärung, in: Hill/Martini/Wagner (Hrsg.), Facebook, Google & Co., 2013, 143 ff.

[56] *Beuth*, Datensammelwut als Spiel, 28.3.2012.

[57] So auch: *Wagner*, Datenschutz als Bildungsauftrag, DuD 2012, 83, 85.

[58] Siehe unten Kapitel 7,A.IV.

[59] Einen solchen Schritt erwägt *Schmies* im Rahmen von Aufklärungspflichten im Finanzmarktrecht: *Schmies*, Behavioral Finance und Finanzmarktregulierung, in: Engel/Englerth/Lüdemann u. a. (Hrsg.), Recht und Verhalten, 2007, 179.

C. Entscheidungsarchitekturen

Derzeit viel diskutiert wird schließlich die Idee des Schutzes durch sogenannte Entscheidungsarchitekturen. Im Folgenden werden ihre Wirkungsweise und die Einsatzmöglichkeiten zur Verhinderung informationeller Preisgabe dargestellt. Die verhaltensökonomische Begründung sowie deren rechtliche Bewertung folgen im weiteren Verlauf der Arbeit.[60]

Erkenntnisse der Verhaltenspsychologie zeigen, dass sich Menschen vorhersehbar irrational entscheiden.[61] Rationale Entschlussfassungen werden angesichts der zu großen Komplexität der Aufgabenstellungen durch den Einsatz von vereinfachenden Gedankenmodellen, Annäherungsstrategien und heuristischem Verhalten ersetzt.[62] Heuristiken sind dabei oft einfache und simple Techniken, die beim Lern- oder Problemlösungsprozess helfen.[63] Die Kenntnis dieser Irrationalitäten kann ausgenutzt werden, um die Nutzer durch bestimmte Gestaltungen der Entscheidungssituation zum Fällen der staatlicherseits gewünschten Entscheidung zu bewegen.[64] Der Staat wird zum Entscheidungsarchitekten,[65] indem er sogenannte Nudges, im Deutschen übersetzbar als „Schubser", gibt.[66] Der Einsatz von Entscheidungsarchitekturen ist dabei umso effektiver, je mehr diese aufgrund vorangegangener Datenanalyse auf die konkreten Nutzer angepasst werden können.[67]

Die Wirkungsweise von Entscheidungsarchitekturen soll im Folgenden am Beispiel von Standardvorgaben (siehe I), Feedback (siehe II), Anreizen zum informationellen Selbstschutz (siehe III), Framing (siehe IV), Ankern (siehe V) und der Erhöhung von Transaktionskosten (siehe VI) erläutert werden.

---

[60] Siehe unten Kapitel 7,A.

[61] Der Ausdruck „predictably irrational" wurde geprägt durch: *Ariely*, Predictably irrational, ²2010; umfassend dazu: *Kahneman*, Thinking, Fast and Slow, 2011.

[62] *Acquisti/Grossklags*, What Can Behavioral Economics Teach us about Privacy?, in: Acquisti/Gritzalis/Lambrinoudakis u. a. (Hrsg.), Digital privacy, 2008, 363, 364, 369.

[63] *Acquisti/Grossklags*, What Can Behavioral Economics Teach us about Privacy?, in: Acquisti/Gritzalis/Lambrinoudakis u. a. (Hrsg.), Digital privacy, 2008, 363, 370; grundlegend der Sammelband: *Kahneman/Slovic/Tversky* (Hrsg.), Judgement under uncertainty, 1982.

[64] In der Literatur wird ein solches Vorgehen überwiegend für sehr erfolgsversprechend gehalten. Eine der wenigen zurückhaltenden Stimmen ist: *Willis*, When Nudges Fail, 80 Chicago L. Rev. (2013), 1115 ff. und *dies.*, Why not Privacy by Default?, 29 Berkeley Tech. L. J. (2014).

[65] *Thaler/Sunstein*, Nudge, ²2012, 11.

[66] Den Begriff führen *Thaler* und *Sunstein* in ihrem Werk „Nudge" ein: *Thaler/Sunstein*, Nudge, ²2012, 106. Dieses wird mitunter als die Bibel der Verhaltensökonomie bezeichnet: *Kahneman*, Thinking, Fast and Slow, 2011, 412; zum Schutz der Privatheit durch Nudges, siehe auch: *Kapsner/Sandfuchs*, Nudging as a Threat to Privacy, 6 Rev. of Philosophy and Psychology (2015), 455 ff.; *dies.*, Coercing Online Privacy, 11 I/S: A Journal of Law and Policy for the Information Society (2016) (im Erscheinen); *Sandfuchs*, Privacy Nudges, in: Akrivopoulou (Hrsg.), Protecting the Genetic Self from Biometric Threats, 2015, 256 ff.

[67] Dazu ausführlich: *Porat/Strahilevitz*, Personalizing Default Rules and Disclosure with Big Data, 112 Mich. L. Rev. (2014), 1417 ff. Einem solchen Vorgehen stehen jedoch erhebliche Privatheitsbedenken entgegen, da es eine umfassende Auswertung von Nutzerdaten erfordert.

I. Standardvorgaben

Verhaltensökonomen nehmen unter dem Begriff der Verlustaversion an, dass es doppelt so unangenehm ist, etwas zu verlieren als der Gewinn dieses Etwas glücklich macht.[68] Die Rede ist auch von Besitzeffekten.[69] So bekam in einem Experiment die Hälfte der Teilnehmer einen Kaffeebecher, die andere Hälfte eine Tafel Schokolade. Der Wert war jeweils identisch und in einer vorangegangenen Befragung gab jeweils circa die Hälfte der Teilnehmer an, einen der beiden Gegenstände lieber haben zu wollen. Doch von der nun gegebenen Gelegenheit, Tasse gegen Schokolade zu tauschen, machten nur zehn Prozent Gebrauch.[70] Der Rest verzichtete auf den Tausch, obwohl dies offensichtlich dem vorher geäußerten Interesse vieler Probanden widersprach.

Menschen neigen weiter dazu, sich dem Verhalten der Mehrheit anzupassen, auch wenn dieses von der eigenen Überzeugung abweicht. So belegen 130 Studien in 17 Ländern, dass 20 bis 40 Prozent der Versuchsteilnehmer auch ganz einfache Fragen falsch beantworten, wenn zuvor alle anderen Teilnehmer die Frage hörbar falsch beantwortet haben.[71] Dieses Phänomen scheint sich auch bei der Entscheidung zur Nutzung sozialer Netzwerke zu zeigen, wie überspitzt am Beispiel des sozialen Netzwerks Facebook ausgeführt wird. „When our friends all jump off the Facebook privacy bridge, we do too. Those behind us figure we wouldn't have jumped unless it was safe, and the Cycle repeats."[72]

Damit im Zusammenhang steht die Tendenz zum Status quo. Menschen verhalten sich träge und ziehen die vorgegebene Option der Veränderung vor.[73] Dies kann im Privatheitskontext dazu führen, dass standardisierte Einwilligungserklärungen und Formate von Nutzern angenommen werden ohne Rücksicht auf ihre persönlichen Präferenzen.[74] In einer Ende 2010 im Auftrag der Europäischen Kommission durchgeführten Befragung von 26.574 EU-Bürgern gaben 55 Prozent der befragten Deutschen an, noch nie versucht zu haben, die Privatheitseinstellung ihrer Accounts in sozialen Netzwerken zu ändern.[75] Auch wenn dieser Studie sicherlich nur noch bedingte Aussagekraft über das heutige Nutzungsverhalten der Bürger zukommt, macht sie doch einen gewissen Hang zum Status quo deutlich.

---

68 *Thaler/Sunstein*, Nudge, ²2012, 53 f.

69 *Eidenmüller*, Liberaler Paternalismus, JZ 2011, 814, 817.

70 *Thaler/Sunstein*, Nudge, ²2012, 54 f.

71 Zitiert nach: *Thaler/Sunstein*, Nudge, ²2012, 84.

72 *Grimmelmann*, Saving Facebook, 94 Iowa L. Rev. (2009), 1137, 1161.

73 *Eidenmüller*, Liberaler Paternalismus, JZ 2011, 814, 818; *Sunstein/Thaler*, Libertarian Paternalism is Not an Oxymoron, 70 Chicago L. Rev. (2003), 1159, 1174 ff. und *dies.*, Nudge, ²2012, 18, 123 ff.

74 *Schwartz*, Beyond Lessig's Code for Internet Privacy, Wisconsin L. Rev. 2000, 743, 768; *ders.*, Internet Privacy and the State, 32 Connecticut L. Rev. (2000), 815, 822 f.; *ders.*, Property, Privacy, and Personal Data, 117 Harvard L. Rev. (2004), 2055, 2081 f. und *Sunstein*, The Storrs Lectures, 122 Yale L. J. (2013), 1826, 1893.

75 *Europäische Kommission*, Special Eurobarometer 359, 6.2011, 164.

Um die Wahrscheinlichkeit zu erhöhen, dass Nutzer die staatlich gewünschte Entscheidung treffen, können entsprechende Standardvorgaben gesetzt werden.[76] Beispiele hierfür sind Art. 23 Abs. 2 EU-DS-GVO-E, der die Verpflichtung zu datenschutzfreundlichen Voreinstellungen beinhaltet sowie der nicht verabschiedete Entwurf des § 13a Abs. 1 Satz 1 und 3 TMG.[77] Nach Letzterem sollten Anbieter von Telemediendiensten mit nutzergenerierten Inhalten verpflichtet werden, die Sicherheitseinstellungen auf höchster Stufe voreinzustellen. Zudem sollten gemäß der Voreinstellung die Nutzerkonten sowie von den Nutzern erstellte Inhalte nicht durch externe Suchmaschinen auffindbar sein. § 13a Abs. 1 Satz 5 TMG-E sollte die Vorgabe ergänzen um eine Form des aufgezwungenen Schutzes. Demnach sollte Nutzern, die bei der Erhebung ihrer personenbezogenen Daten ein Alter von unter 16 Jahren angegeben hatten, eine Änderung der Voreinstellungen erst ermöglicht werden, wenn sie das Alter von 16 Jahren erreichen.

II. Feedback

Die Fehlerquote bei Entscheidungen kann gesenkt werden, indem den Nutzern vor und nach der Begehung von Fehlern Rückmeldung gegeben wird.[78]

So testete eine 2012 in den USA durchgeführte Studie verschiedene Methoden, Facebook-Nutzer von der Veröffentlichung von Posts oder Kommentaren abzuhalten, die sie später bereuen würden. Nachdem in einer vorangegangenen Untersuchung festgestellt worden war, dass Nutzer häufig bedauern, ihre Posts zu vielen Adressaten gegenüber kundgetan zu haben, wurden Nutzern vor der Veröffentlichung von Posts oder Kommentaren fünf zufällig ausgewählte Profilfotos anderer Nutzer gezeigt, die diesen Post sehen können würden.[79] Weiter hatte die Voruntersuchung gezeigt, dass Nutzer häufig emotionale Posts bereuen. Daher wurde anderen Teilnehmern der Studie vor dem Veröffentlichen eines emotionalen Posts oder Kommentars für zehn Sekunden ein entsprechender Hinweis gezeigt, zum Beispiel: „Other people might perceive your post as negative".[80] Die Studie erstreckte sich nur auf 21 Teilnehmer und drei Wochen, sodass repräsentative Ergebnisse nicht gewonnen werden konnten. Jedoch zeigt sich, dass beide Feedback-Varianten bei einigen Nutzern zum Nichtveröffentlichen von Posts, Ändern des Adressatenkreises sowie Anpassen der Privatheitseinstellungen führten.[81]

---

[76] *Sunstein*, The Storrs Lectures, 122 Yale L. J. (2013), 1826, 1888 f.

[77] Entwurf eines Gesetzes zur Änderung des Telemediengesetzes, BT-Drs. 17/6765 v. 3.8.2011.

[78] *Thaler/Sunstein*, Nudge, ^{2}2012, 131 f.

[79] *Wang/Leon/Chen u. a.*, From Facebook Regrets to Facebook Privacy Nudges, 74 Ohio State L. J. (2013), 1307, 1321.

[80] *Wang/Leon/Chen u. a.*, From Facebook Regrets to Facebook Privacy Nudges, 74 Ohio State L. J. (2013), 1307, 1322.

[81] *Wang/Leon/Chen u. a.*, From Facebook Regrets to Facebook Privacy Nudges, 74 Ohio State L. J. (2013), 1307, 1327 ff.

III. Anreize zum informationellen Selbstschutz

Entscheidungsfindung wird durch Heuristiken beeinflusst. Die Einschätzung der Wahrscheinlichkeit des Eintritts eines Risikos kann dadurch gelenkt werden, wie schnell den Nutzern entsprechende Beispiele einfallen (sogenannte Heuristik nach Verfügbarkeit).[82] Es zeigt sich auch, dass Menschen systematisch gleich intensive zeitlich nahe und ferne Folgen unterschiedlich stark gewichten.[83] Nehmen privatheitsschätzende Nutzer kostenfreie Möglichkeiten zur privatheitswahrenden Internetnutzung nicht in Anspruch oder geben sie ihre Daten im Tausch gegen geringfügige aktuelle Vorteile auf, kann ein Fall eines solchen vorhersehbaren Unterschätzens zukünftiger negativer Konsequenzen und des Bevorzugens unmittelbarer Gratifikation vorliegen.[84] Hinzu tritt der sogenannte Optimismus-Bias, nach dem Menschen systematisch die Wahrscheinlichkeit des Eintritts positiver Ereignisse über-, und des Eintritts negativer Ereignisse unterschätzen.[85] Demnach gehen Viele davon aus, dass positive Ereignisse bei ihnen selbst häufiger eintreten als bei Anderen. Im Kontext sozialer Netzwerke zeigt sich, dass Nutzer zwar vom Vorhandensein von Datenschutzproblemen wissen, jedoch regelmäßig nicht erwarten, selbst davon betroffen zu sein.[86] Ist eine Gefahr schwer vorstellbar, wie beispielsweise ein Identitätsdiebstahl, wird die Wahrscheinlichkeit ihres Eintritts unterschätzt (sogenannte Simulationsheuristik).[87]

Die Entscheidungsfehler hinsichtlich zu weitreichender informationeller Preisgabe können ausgeglichen und unter Umständen sogar ausgenutzt werden, um informationelle Preisgabe zu verhindern. Es bietet sich an, Maßnahmen zu ergreifen, um die Aufmerksamkeit der Menschen auf bestimmte Umstände zu lenken.[88]

So kann als Offline-Beispiel eine gesündere Ernährung von Schulkindern erreicht werden, wenn in Schulcafeterien die Speisen dergestalt angeordnet werden, dass Obst und Gemüse zuerst angeboten werden, während beispielsweise zucker-

---

[82] *Sunstein*, The Storrs Lectures, 122 Yale L. J. (2013), 1826, 1851 f. und *Thaler/Sunstein*, Nudge, ²2012, 42 ff.

[83] *Sunstein*, The Storrs Lectures, 122 Yale L. J. (2013), 1826, 1842 ff.

[84] *Acquisti*, Privacy in Electronic Commerce and the Economics of Immediate Gratification, in: Breese (Hrsg.), Proceedings of the 5th ACM Conference on Electronic Commerce, 2004, 21, 24 ff.; *Acquisti/Grossklags*, What Can Behavioral Economics Teach us about Privacy?, in: Acquisti/Gritzalis/Lambrinoudakis u. a. (Hrsg.), Digital privacy, 2008, 363, 371 f.; *Jolls*, Rationality and Consent in Privacy Law. 2010, 49 f.; vgl.: *Acquisti/Grossklags*, Privacy and Rationality in Individual Decision Making, 2005, 9.

[85] *Sunstein*, The Storrs Lectures, 122 Yale L. J. (2013), 1826, 1848 ff.

[86] *Acquisti/Gross*, Imagined Communities 2006, 13 f.; *Acquisti*, Privacy in Electronic Commerce and the Economics of Immediate Gratification, in: Breese (Hrsg.), Proceedings of the 5th ACM Conference on Electronic Commerce, 2004, 21, 24 und *Jolls*, Rationality and Consent in Privacy Law, 2010, 42 ff.

[87] *Acquisti/Grossklags*, What Can Behavioral Economics Teach us about Privacy?, in: Acquisti/Gritzalis/Lambrinoudakis u. a. (Hrsg.), Digital privacy, 2008, 363 ff.

[88] *Thaler/Sunstein*, Nudge, ²2012, 143.

haltige Nachspeisen aus einem Nebenraum geholt werden müssen.[89] Ebenso kann der Staat den „Preis" eines Verhaltens ändern, indem er ihn etwa durch Auflagen oder steuerliche Belastungen erhöht. Beispiele hierfür sind die Kraftfahrzeug-Nutzung sowie der Tabak- und Alkoholkonsum.[90]

Im Internetkontext können abschreckende Methoden eingesetzt werden, um den Nutzern das Vorhandensein digitaler Überwachung bemerkbar zu machen. So können Webseiten, die das Nutzerverhalten speichern, verpflichtet werden, einen die Nutzer verfolgenden Avatar anzuzeigen. Durch einen Klick können die Nutzer diesen ausblenden oder aber ihr Opt-out aus dem Tracking erklären.[91]

IV. Framing

Das Framing, also die Art und Weise, wie eine Frage oder verschiedene Entscheidungsoptionen präsentiert werden, beeinträchtigt das erzielte Resultat.[92] In einer Studie wurde beispielsweise Rindfleisch, das als „75 Prozent mager" gekennzeichnet war, als magerer, von höherer Qualität, weniger fettig und besser schmeckend bewertet als Rindfleisch, das mit dem Attribut „25 Prozent Fett" versehen war.[93] Die Option „Click here for continuous surveillance" wird entsprechend weniger Zuspruch finden als die Option „Click here for more relevant advertising".[94]

Ein Fall der Repräsentativitäts-Heuristik liegt vor, wenn Entscheidungen über die Vertrauenswürdigkeit von Anbietern durch ansprechendes Website-Design geprägt werden.[95] So kreiert beispielsweise das Design des sozialen Netzwerks Facebook ein intimes, vertrauliches und sicheres Umfeld.[96]

Die Erkenntnisse über die Wirkung von Framing können ausgenutzt werden, um trotz gleichbleibenden Inhalts durch kleine Änderungen in der Präsentation eines Angebots die Nutzer zur Preisgabe von weniger personenbezogenen Daten zu bewegen.[97] So können durch das Design von Webseiten das Unterschätzen von Risiken sowie die Preisgabe personenbezogener Daten limitiert werden.

---

89 *Thaler/Sunstein*, Nudge, ²2012, 1 f.

90 *Littwin*, Grundrechtsschutz gegen sich selbst, 1993, 238.

91 *Calo*, Against Notice Skepticism in Privacy (and Elsewhere), 87 Notre Dame L. Rev. (2012), 1027, 1040 (der dieses Mittel jedoch als „visceral notice" einstuft, also als alternative Unterrichtungsmethode, vgl.: oben Kapitel 4,B.II).

92 *Eidenmüller*, Liberaler Paternalismus, JZ 2011, 814, 817; *Sunstein/Thaler*, Libertarian Paternalism is Not an Oxymoron, 70 Chicago L. Rev. (2003), 1159, 1179 f. und *dies.*, Nudge, ²2012, 57 ff.

93 *Levin/Gaeth*, How Consumers Are Affected by the Framing of Attribute Information Before and After Consuming a Product, 15 J. of Consumer Research (1988), 374, 376 ff.

94 *Zuiderveen Borgesius*, Improving Privacy Protection in the Area of Behavioural Targeting, 2015, 236.

95 *Acquisti/Grossklags*, What Can Behavioral Economics Teach us about Privacy?, in: Acquisti/Gritzalis/Lambrinoudakis u. a. (Hrsg.), Digital privacy, 2008, 363, 371.

96 *Grimmelmann*, Saving Facebook, 94 Iowa L. Rev. (2009), 1137, 1160, 1162 f.

97 *Acquisti/Grossklags*, Uncertainty, Ambiguity and Privacy, 6.3.2005, 15 ff.

V. Anker

Weiter können gezielt Anker eingeführt werden, um die Entscheidungsfindung der Nutzer zu beeinflussen.[98] Um Unbekanntes kalkulieren zu können, setzen Menschen Anker bei Fakten, die sie kennen und versuchen, auf dieser Basis die Antwort zu finden.[99] Dabei wird jedoch systematisch eine zu geringe Anpassung vorgenommen. So schätzen Bewohner einer Großstadt benachbarte mittelgroße Städte als zu groß ein, während Bewohner einer Kleinstadt sie als zu klein einschätzen.[100] Dabei können sogar vollständig irrelevante Fakten als Anker dienen, wie die letzten drei Ziffern der Telefonnummer oder die letzten zwei Ziffern der Sozialversicherungsnummer.[101]

Im Privatheitskontext ist anzunehmen, dass sich Nutzer zur Beantwortung der schwierigen Frage nach dem Wert ihrer Daten geeignet erscheinender Anker bedienen und sich an diesen bei zukünftigen Entscheidungen über ihre informationelle Preisgabe orientieren.[102] Durch Einsetzen von hohen Ankern können Nutzer dazu gebracht werden, den Wert ihrer Privatheit hoch einzuschätzen.

VI. Erhöhung der Transaktionskosten und Wartezeiten

Schließlich können Nutzer durch eine strategische Anpassung der Transaktionskosten von unerwünschtem Verhalten abgehalten werden. So kann beispielsweise für die Preisgabe regulärer personenbezogener Daten ein Mausklick ausreichend sein, während für die Preisgabe sensibler Daten mehrere Mausklicks oder eine zeit- und kostenintensive Einwilligungserklärung auf dem Postweg erforderlich sind.[103]

Nutzer können weiter vor übereilten Entscheidungen bewahrt werden, indem ihnen eine Cooling-off-Period, also eine verpflichtende Bedenkzeit, auferlegt wird, bevor Entscheidungen ausgeführt werden. Wartezeiten, in denen eine getroffene Entscheidung noch nicht umgesetzt werden kann, lassen sich dabei als Weiterentwicklung von Widerrufsrechten sehen. Letztere schließen zwar die sofortige Implementierung der Entscheidung nicht aus, gewähren aber dennoch eine Bedenkzeit. Als Offline-Beispiel wird eine verpflichtende Trennungszeit, deren Ablauf Voraussetzung für eine Ehescheidung ist, genannt.[104]

---

98 *Sunstein/Thaler*, Libertarian Paternalism is Not an Oxymoron, 70 Chicago L. Rev. (2003), 1159, 1177 f.

99 *Eidenmüller*, Liberaler Paternalismus, JZ 2011, 814, 817 und *Thaler/Sunstein*, Nudge, ^{2}2012, 39 ff.

100 *Thaler/Sunstein*, Nudge, ^{2}2012, 39 ff.

101 *Ariely*, Predictably irrational, ^{2}2010, 28.

102 *Acquisti/Grossklags*, What Can Behavioral Economics Teach us about Privacy?, in: Acquisti/Gritzalis/Lambrinoudakis u. a. (Hrsg.), Digital privacy, 2008, 363, 370 f.

103 *Zuiderveen Borgesius*, Consent to Behavioural Targeting in European Law, 7.2013, 56.

104 *Sunstein/Thaler*, Libertarian Paternalism is Not an Oxymoron, 70 Chicago L. Rev. (2003), 1159, 1187 f. Das Trennungsjahr wird im deutschen Recht umgesetzt durch § 1565 Abs. 2 BGB.

Ausgehend von der Feststellung, dass Facebook-Nutzer häufig übereilte Posts bereuen, erlegte die bereits angesprochene, 2012 in den USA durchgeführte Studie Facebook-Nutzern eine Bedenkzeit[105] von zehn Sekunden auf, bevor sie Posts oder Kommentare veröffentlichen konnten.[106] Hierbei konnten die Nutzer entweder abwarten, den Post editieren, ihn löschen oder ihn sofort veröffentlichen. Dies führte bei einigen Nutzern zum Abändern oder Nicht-Veröffentlichen von Posts.[107]

Auch kann die informationelle Preisgabe mit monetären Kosten versehen werden. Menschen neigen zu einer irrationalen Bevorzugung kostenfreier Produkte. Selbst wenn der Erwerb eines kostenpflichtigen besseren Produkts im Interesse der Individuen läge, entscheiden sie sich regelmäßig für das kostenlose Produkt. „Zero is an emotional hot button – a source of irrational excitement."[108] Diesen Effekt demonstriert eine Studie, bei der die Teilnehmer die Wahl hatten zwischen einem kostenlosen 10-Dollar-Einkaufsgutschein für den Internet-Versandhandel Amazon und dem Kauf eines 20-Dollar-Gutscheins zum Preis von sieben Dollar. Der Großteil der Teilnehmer entschied sich für den kostenlosen Gutschein. Im Anschluss wurde den Teilnehmern der 10-Dollar-Gutschein für einen Dollar zum Kauf angeboten, der 20-Dollar-Gutschein für acht Dollar. Obwohl beide Preise einheitlich um einen Dollar erhöht wurden, entschied sich nun die Mehrheit für den 20-Dollar-Gutschein.[109]

Durch staatliche Vorgaben, die beispielsweise eine Einwilligung auf dem Postweg vorschreiben und damit regelmäßig Portokosten anfallen lassen, kann kostenlosen Online-Produkten ein Teil ihres Reizes genommen werden.

---

[105] Zur Idee der aufgezwungenen Wartezeit schon: *Dworkin*, Paternalism, in: Sartorius (Hrsg.), Paternalism, 1983, 19, 32.

[106] *Wang/Leon/Chen u. a.*, From Facebook Regrets to Facebook Privacy Nudges, 74 Ohio State L. J. (2013), 1307, 1321 f.

[107] *Wang/Leon/Chen u. a.*, From Facebook Regrets to Facebook Privacy Nudges, 74 Ohio State L. J. (2013), 1307, 1328 f.; allgemein zur Selbstzensur hinsichtlich der Veröffentlichung von Posts in sozialen Netzwerken: *Das/Kramer*, Self-Censorship on Facebook, in: Kiciman/Ellison/Hogan u. a. (Hrsg.), Proceedings of the Seventh International AAAI Conference on Weblogs and Social Media, 2013, 120 ff.

[108] *Ariely*, Predictably irrational, ^{2}2010, 55 ff.

[109] *Ariely*, Predictably irrational, ^{2}2010, 64.

Kapitel 5

Pflicht zur Verhinderung der Preisgabe

Es stellt sich die Frage nach der Existenz einer staatlichen Pflicht zur Verhinderung informationeller Preisgabe, um den Gefahren zu begegnen, die informationelle Preisgabe für verfassungsrechtlich geschützte Interessen der Preisgebenden und der Allgemeinheit in Deutschland und in den Vereinigten Staaten mit sich bringen kann.

Sowohl die Pflicht als auch die Befugnis zur Verhinderung selbstgefährdenden Verhaltens werden in der Literatur häufig ohne weitere Begründung im Rahmen der Schutzpflichtendogmatik diskutiert.[1]

Zwingend ist diese Einordnung jedoch keineswegs. An anderer Stelle wird richtigerweise zwischen „Schutzpflicht" und „Schutzberechtigung" differenziert und darauf hingewiesen, dass genau genommen nach einem „Grundrechtsschutzgüter-Schutz gegen sich selbst" gefragt werden müsste.[2] Da es Konstellationen gibt, in denen der Staat zwar nicht zum Schutz der Selbstgefährdenden vor sich selbst verpflichtet ist, aber sie dennoch schützen darf, muss unterschieden werden zwischen der in diesem Kapitel analysierten Schutzpflicht und der im nächsten Kapitel untersuchten Befugnis zum Schutz vor sich selbst.

Zunächst werden Existenz und Umfang verfassungsrechtlicher Pflichten zur Verhinderung informationeller Preisgabe nach deutschem (siehe A) und US-amerikanischem Verfassungsrecht analysiert (siehe B).

A. Schutzpflicht nach dem Grundgesetz

Überwiegen die Gefahren der informationellen Preisgabe ihren Nutzen, stellt sich die Frage nach einer grundrechtlichen Pflicht zur Verhinderung informationeller Preisgabe.

Im Folgenden soll dargestellt werden, wie sich aus der objektiv-rechtlichen Grundrechtsdimension (siehe I) eine grundrechtliche Schutzpflichtendimension entwickelte (siehe II), wann eine Schutzpflicht entsteht (siehe III) und was bei ihrer Umsetzung zu beachten ist (siehe IV). Im Anschluss werden die Erkenntnisse auf

---

[1] So wohl: *Münch*, Grundrechtsschutz gegen sich selbst?, in: Stödter/Thieme (Hrsg.), Festschrift für Hans Peter Ipsen zum siebzigsten Geburtstag, 1977, 113, 114: kritisch jedoch: *Hillgruber*, Der Schutz des Menschen vor sich selbst, 1992, 147 f.

[2] *Schwabe*, Der Schutz des Menschen vor sich selbst, JZ 1998, 66, 70. 67.

die Frage angewandt, ob und wann eine Pflicht zur Verhinderung informationeller Preisgabe besteht (siehe V, VI, VII und VIII).

I. Objektiv-rechtliche Grundrechtsdimension

Grundrechte kommen – entgegen der Auffassung *Nipperdeys*[3] – zwischen Privaten nicht direkt zur Anwendung (keine unmittelbare Drittwirkung), wie der Wortlaut des Art. 1 Abs. 3 GG und ein Umkehrschluss aus Art. 9 Abs. 3 Satz 2, 20 Abs. 4 und 48 Abs. 2 Satz 2 GG, die in Ausnahmefällen eine unmittelbare Drittwirkung anordnen, belegen. Vielmehr sind Private jeweils selbst grundrechtsberechtigt. Dennoch besteht eine mittelbare grundrechtliche Drittwirkung zwischen ihnen.[4]

Ob es dieser Konstruktion tatsächlich bedarf, wird zwar von *Schwabe* angezweifelt, da der Staat auch ohne die „sogenannte Drittwirkung"[5] bei der Regelung von Privatrechtsverhältnissen gemäß Art. 1 Abs. 3 GG direkt an die Grundrechte gebunden sei.[6] Dem ist jedoch entgegenzuhalten, dass der Staat zwar bei der Ausgestaltung der Verhältnisse Privater zueinander deren Grundrechte zu beachten hat, diese jedoch in einen schonenden Ausgleich bringen muss, der in dieser Form mangels widerstreitender grundrechtlicher Interessen im Staat-Bürger-Verhältnis nicht zu erzielen ist. Die Kategorie der mittelbaren grundrechtlichen Drittwirkung besitzt damit eine eigenständige Berechtigung.

Grundrechte stellen, nach der so nicht mehr verwendeten frühen Formulierung des Bundesverfassungsgerichts, eine objektive Wertordnung dar, die als verfassungsrechtliche Grundentscheidung für alle Bereiche des Rechts gilt.[7] Um dieser

---

[3] *Nipperdey*, Grundrechte und Privatrecht, 1961, 14 ff., ebenso das Bundesarbeitsgericht in der Frühzeit seiner Rechtsprechung, siehe: BAGE 1, 185 und 1, 258.

[4] Entwickelt von *Dürig* in Reaktion auf *Nipperdeys* Theorie von der unmittelbaren Grundrechtswirkung zwischen Privaten: *Dürig*, Grundrechte und Privatrechtsprechung, in: Maunz (Hrsg.), Vom Bonner Grundgesetz zur gesamtdeutschen Verfassung, 1956, 157, 176 ff., aufgegriffen durch: BVerfGE 7, 198 (205 ff.); 25, 256 (263); 30, 173 (188); 34, 269 (280); 42, 133 (139); 42, 143 (147 f.) und 54, 148 (151 f.). Umfassende dogmatische Aufarbeitungen bieten unter anderem: *Langner*, Die Problematik der Geltung der Grundrechte zwischen Privaten, 1998, 55 ff.; *Leisner*, Grundrechte und Privatrecht, 1960, 285 ff. und *Papier*, Drittwirkung der Grundrechte, in: Merten/Papier (Hrsg.), Handbuch der Grundrechte in Deutschland und Europa II, 2006, 1331, 1332 ff., Rn. 1 ff.

[5] So bereits der Titel von *Schwabes* Monographie: *Schwabe*, Die sogenannte Drittwirkung der Grundrechte, 1971.

[6] *Schwabe* kritisiert die herrschende Meinung daher scharf: „Wenn demnach diese Privatrechtsgeltung der Grundrechte insoweit ohne sachliche Bedeutung ist, muß mehr als fraglich erscheinen, ob ihre Durchsetzung Ströme von Tinte und Unmengen an Druckerschwärze lohnt. Nicht nur von der Ökonomie her will nicht recht einleuchten, weshalb die den subjektiv-privaten Grundrechten hinderlichen Hürden, insbesondere die des Art. 1 Abs. 3 GG, mit recht aufwendig vorbereiteten und mitunter sehr kühn anmutenden Geistessprüngen überwunden werden sollen, wenn es das Reglement zumindest gestattet und […] sogar gebietet, diese Hürde seitlich zu passieren.", *Schwabe*, Die sogenannte Drittwirkung der Grundrechte, 1971, 140 f.

[7] BVerfGE 7, 198 (205); zur Entwicklung des Konstrukts der „objektiven Wertordnung": *Hornung*, Grundrechtsinnovationen, 2015, 240 ff.

Grundentscheidung Rechnung zu tragen, ist das Recht insgesamt im Lichte der Grundrechte auszulegen. Davon erfasst ist auch das Zivilrecht, das das Verhältnis zwischen Privaten regelt. Die Rede ist nun von einer objektiv-rechtlichen Dimension der Grundrechte. Insbesondere kommt dieser Grundrechtsdimension eine Bedeutung zu bei der Auslegung von Generalklauseln und unbestimmten Rechtsbegriffen. Gesetzgebung, Verwaltung und Rechtsprechung empfangen Impulse und Richtlinien von den Grundrechten.[8] Aufgrund dieser grundrechtlichen „Ausstrahlungswirkung"[9] müssen die durch informationelle Preisgabe bedrohten Rechtsgüter – also das Recht auf informationelle Selbstbestimmung und die Informationsfreiheit – bei der Auslegung von zwischen Privaten geltenden Gesetzen berücksichtigt werden.

II. Herleitung der Schutzpflicht

Auf dieser Basis entwickelte sich die Dogmatik der Schutzpflichtendimension der Grundrechte.[10] Im Ausgangspunkt kommt Grundrechten eine liberale, subjektivrechtlich fundierte Funktion als Abwehrrechte der Bürger gegen den Staat zu. Die Bürger sollen ihr Leben frei von ungerechtfertigten staatlichen Eingriffen führen können.

Doch Bedrohungen für grundrechtlich geschützte Interessen der Bürger gehen nicht nur von staatlicher Seite, sondern auch von nicht-staatlichen Akteuren aus. Dabei kann es sich sowohl um natürliche als auch um juristische Personen handeln. In Anlehnung an die treffende, in der Literatur verbreitete Terminologie werden Beeinträchtigungen grundrechtlich geschützter Rechtsgüter durch Dritte im Rahmen dieser Arbeit nicht als Eingriff, sondern als Übergriff bezeichnet.[11] Die Behandlung derartiger Dreieckskonstruktionen wirft Schwierigkeiten auf:

---

[8] BVerfGE 7, 198 (205).

[9] BVerfGE 7, 198 (205).

[10] Den Grundstein hierfür legte: *Canaris*, Grundrechte und Privatrecht, 184 AcP (1984), 201, 212 ff.; zur verfassungsgerichtlichen Entwicklung der Schutzpflichten: *Hornung*, Grundrechtsinnovationen, 2015, 248 ff.; für einen Überblick sei statt vieler verwiesen auf: *Calliess*, Schutzpflichten, in: Merten/Papier (Hrsg.), Handbuch der Grundrechte in Deutschland und Europa II, 2006, 963, 964 ff., Rn. 1 ff. *Rupp* lieferte jüngst eine ausführliche Untersuchung der Entwicklung der Schutzpflichtendogmatik: *Rupp*, Die grundrechtliche Schutzpflicht des Staates für das Recht auf informationelle Selbstbestimmung im Pressesektor, 2013. Aktuell mit den Schutzpflichten im Internet befassen sich: *Schliesky/Hoffmann/Luch u. a.*, Schutzpflichten und Drittwirkung im Internet, 2014, 47 ff., 98 ff.; dazu: *Sandfuchs*, Rezension, MMR-Aktuell 2015, 365281. Eine englischsprachigen Überblick bieten: *Graßhof*, The Duty to Protect and to Ensure Human Rights and the Basic Law of the Federal Republic of Germany, in: Klein (Hrsg.), The Duty to Protect and to Ensure Human Rights, 2000, 33 ff. und *Sachs*, The Duty to Protect and to Ensure Human Rights Under the Basic Law of the Federal Republic of Germany, in: Klein (Hrsg.), The Duty to Protect and to Ensure Human Rights, 2000, 53 ff.

[11] *Isensee*, Das Grundrecht auf Sicherheit, 1983, 44 und *Krings*, Grund und Grenzen grundrechtlicher Schutzansprüche, 2003, 27 m. w. N.

Jedenfalls trifft den Staat eine Handlungspflicht, wenn ihm eine Garantenstellung für das Verhalten Dritter zukommt. Dies ist der Fall, wenn der Staat besondere Angriffsmöglichkeiten oder -anreize geschaffen hat, beispielsweise durch Verpflichtung der Zeugen zur Aussage in einem Strafprozess.[12]

Auch steht er in der Pflicht, wenn ihm das Verhalten der Privaten ausnahmsweise zugerechnet werden kann. Zu denken ist an Fälle, in denen der Staat das in Rede stehende Verhalten anregt oder fördert, sodass die Konstellation eines mittelbaren Eingriffs vorliegt. Teilweise wird unterteilt in Zweckveranlassung (die Privaten sind Helfer des Staates oder die Beeinträchtigung ist zwangsläufige Folge einer staatlichen Maßnahme), Erlaubnis, Anregung und Duldung, wobei ein Grundrechtseingriff nur dann vorliegt, wenn der staatliche Einfluss derart konstitutiv ist, dass seine Unterlassung die Beeinträchtigung beseitigen oder unmöglich machen würde.[13] Diese Einteilung ermöglicht eine sinnvolle Kategorisierung der denkbaren Konstellationen eines mittelbaren Eingriffs. Die Zurechenbarkeit der Beeinträchtigung zum Staat ist im Übrigen auch der einzige Fall, in dem das US-Verfassungsrecht ein staatliches Einschreiten zwischen Privaten fordert (dann liegt ein Fall der sogenannten State Action vor).[14]

Abgesehen von diesen eher seltenen Konstellationen, stellt sich die Frage, ob und inwieweit vom Staat ein Tätigwerden zu verlangen ist, wenn grundrechtlich geschützte Interessen durch das Verhalten privater Dritter beeinträchtigt werden. Private sind selbst grundrechtsberechtigt, nicht jedoch -verpflichtet. Gleichwohl können sie grundrechtlich geschützte Güter der Einzelnen in einer Weise bedrohen, die Anlass zu staatlichem Eingreifen zu bieten scheint. So ist zu klären, ob Grundrechten auch eine Pflicht zu vorbeugendem, kurativem oder bestrafendem Einschreiten des Staates entnommen werden kann, sodass der Staat zur Intervention in den Konflikt zwischen Privaten verpflichtet ist.

Losgelöst von den Worten des Grundgesetzes, lässt sich eine Schutzpflicht auf staatstheoretische Ansätze stützen. Demnach beruht die Anerkennung von Schutzpflichten nicht erst auf einer Verfassung, sondern auf dem Staatszweck als solchem.[15] *Hobbes* beschreibt einen Naturzustand der Menschen, in dem sie zwar frei sind, jedoch Übergriffe anderer ebenso freier Menschen fürchten müssen.[16] Um

---

[12] BGH NStZ 1984, 31, 32; weitere Beispiele: *Dietlein*, Die Lehre von den grundrechtlichen Schutzpflichten, 1992, 163 ff., vgl.: *Krings*, Grund und Grenzen grundrechtlicher Schutzansprüche, 2003, 27.

[13] *Hermes*, Das Grundrecht auf Schutz von Leben und Gesundheit, 1987, 82 ff.

[14] Siehe unten Kapitel 5,B.

[15] Zum Vertragskonzept von *Hobbes* und der Ergänzung um freiheitliche Aspekte durch *Locke*: *Krings*, Grund und Grenzen grundrechtlicher Schutzansprüche, 2003, 28 ff. und *Schmidt*, Demokratietheorien, [4]2008, 49 ff.; *Krings* weist zudem auf die „historische Unhaltsamkeit" der Vertragskonzepte hin: *Krings*, Grund und Grenzen grundrechtlicher Schutzansprüche, 2003, 38. *Klein* gibt zurecht zu bedenken, dass auch bei Nichteinhaltung des staatlichen Schutzversprechens eine Aufkündigung des Gewaltverzichts vonseiten der Bürger nicht in Betracht kommt: *Klein*, Grundrechtliche Schutzpflicht des Staates, NJW 1989, 1633, 1635 f.

[16] *Hobbes*, Leviathan, 1982 (Original: 1651), Kap. XIV.

diesem kontinuierlichen Kriegszustand zu begegnen, geben alle Menschen Hoheitsrechte an den Souverän ab, der fortan für Sicherheit sorgt. *Hobbes* definiert die Aufgabe des Souveräns so: „to defend them from the invasion of foreigners, and the injuries of one another, and thereby to secure them in such sort as that by their own industry and by the fruits of the earth they may nourish themselves and live contentedly".[17] Im Gegenzug verzichten die Bürger auf Selbstverteidigung. Um diesem Konstrukt gerecht zu werden, muss der Souverän jedoch auch tatsächlich für die Verteidigung der Bürger sorgen.[18] Als Konsequenz der von *Hobbes* begründeten Vertragstheorie kann damit das Bestehen staatlicher Schutzpflichten angesehen werden, um die Sicherheit der Einzelnen zu gewährleisten. Daraus folgt jedoch nicht, dass Schutzpflichten bereits in der abwehrrechtlichen Dimension der Grundrechte enthalten sind.[19]

Nach den Worten *Jellineks* kommt den Grundrechten über den negativen Status[20] hinaus ein positiver Status[21] zu.[22] Der Staat schafft die Bedingungen der Freiheit seiner Bürger. Mit der Anerkennung von Schutzpflichten wird deutlich, dass der positive Status nicht nur Rechte der Bürger beinhaltet, von dem Staat staatliche Leistungen zu verlangen, sondern auch eine Schutzverpflichtung des Staates innerhalb von Privatrechtsverhältnissen. *Isensee* geht dabei soweit, ein subjektiv-rechtliches „Grundrecht auf Sicherheit" zu postulieren.[23]

Das Grundgesetz enthält bestimmte explizite Schutzpflichten. Für die Menschenwürde ergeben sich diese bereits aus dem Wortlaut des Art. 1 Abs. 1 Satz 2, 2. Alt GG („zu schützen"). Art. 6 Abs. 1 GG stellt weiter Ehe und Familie „unter den besonderen Schutz der staatlichen Ordnung". Nach Art. 6 Abs. 2 Satz 2 GG wacht der Staat über die Pflege und Erziehung durch die Eltern und schützt damit die Kinder. Art. 6 Abs. 4 GG enthält einen ausdrücklichen Anspruch der Mutter auf „den Schutz und die Fürsorge der Gemeinschaft". Art. 140 GG in Verbindung mit Art. 139 WRV schützt Sonntage als „Tage der Arbeitsruhe und der seelischen Erhebung".

---

[17] *Hobbes*, Leviathan, 1982 (Original: 1651), Kap. XVII.

[18] *Gusy*, Rechtsgüterschutz als Staatsaufgabe, DÖV 1996, 573, 576 f.

[19] *Calliess*, Schutzpflichten, in: Merten/Papier (Hrsg.), Handbuch der Grundrechte in Deutschland und Europa II, 2006, 963, 973 ff.; *Isensee*, Das Grundrecht als Abwehrrecht und als staatliche Schutzpflicht, in: Isensee/Kirchhof (Hrsg.), Handbuch des Staatsrechts der Bundesrepublik Deutschland X, 2012, 413, 535 ff. und *Stern*, Das Staatsrecht der Bundesrepublik Deutschland III/1, 1988, § 67, V 2, 730 ff.; zum Ausgangspunkt der Debatte: BVerfGE 53, 30 (57 f.).

[20] *Jellinek*, System der subjektiven öffentlichen Rechte, 1892, 89 ff.

[21] *Jellinek*, System der subjektiven öffentlichen Rechte, 1892, 109 ff.

[22] Eine kritische Auseinandersetzung mit *Jellineks* Statuslehre liefert: *Alexy*, Theorie der Grundrechte, 1985, 229 ff.

[23] *Isensee*, Das Grundrecht auf Sicherheit, 1983, 33 ff. Ein solches ist jedoch jedenfalls in der, in der Politik häufig geforderten, Variante eines „Supergrundrechts" auf Sicherheit (*Krempl*, Friedrich erhebt Sicherheit zum „Supergrundrecht", 17.7.2013), das sich gegen alle anderen Grundrechte durchsetzen und damit de facto als Eingriffsrechtfertigung dienen würde, abzulehnen. Wenn man es so bezeichnen möchte, ist der Menschenwürde die Funktion als „Supergrundrecht" vorbehalten. Andere Grundrechte sind der Abwägung zugänglich.

Die Existenz von Schutzpflichten wird auch zugrunde gelegt von diversen Grundrechtsschranken, die sich auf den staatlichen Schutzauftrag beziehen. Art. 5 Abs. 2, 2. Var. GG ermöglicht die Rechtfertigung von Eingriffen zum Schutz der Jugend oder der persönlichen Ehre. Art. 11 Abs. 2 GG lässt Einschränkungen der Freizügigkeit zu zur „Bekämpfung von Seuchengefahr, Naturkatastrophen oder besonders schweren Unglücksfällen, zum Schutze der Jugend vor Verwahrlosung oder um strafbaren Handlungen vorzubeugen". Art. 13 Abs. 4 Satz 1 GG gestattet Eingriffe zur Abwehr einer „gemeinen Gefahr oder einer Lebensgefahr", Art. 13 Abs. 7 GG schließlich spricht von der Abwehr „einer gemeinen Gefahr oder einer Lebensgefahr für einzelne Personen" sowie von Maßnahmen zur „Behebung der Raumnot, zur Bekämpfung von Seuchengefahr oder zum Schutze gefährdeter Jugendlicher".

Auch wenn die Schutzpflichtendimension des Art. 6 GG, des Art. 140 GG in Verbindung mit Art. 139 WRV sowie die Andeutung der Schutzpflichten in diversen Eingriffsbefugnissen nicht verallgemeinerungsfähig sind, geben sie Aufschluss darüber, dass das Grundgesetz Schutzpflichten gewährt. Der Menschenwürdegehalt aller Grundrechte führt dazu, dass auch den übrigen Grundrechten eine Schutzpflichtendimension entnommen werden muss. Weiter wird schließlich das Sozialstaatsprinzip erfüllt, indem der Staat durch schützendes Eingreifen das Verhältnis freier Bürger untereinander reguliert.

Das Bundesverfassungsgericht deutete die Existenz von Schutzpflichten bereits in der Entscheidung zur Hinterbliebenenrente aus dem Jahr 1951[24] und in der ersten Entscheidung zur Adoption aus dem Jahr 1968[25] an. Diese Entscheidungen blieben jedoch für die Entwicklung der Schutzpflichtendogmatik quasi bedeutungslos.

Erstmalige ausdrückliche Anerkennung findet die grundrechtliche Schutzpflicht in der ersten Schwangerschaftsabbruchs-Entscheidung des Bundesverfassungsgerichts aus dem Jahr 1975, in der eine Schutzpflicht hinsichtlich des Rechts auf Leben aus Art. 2 Abs. 2 Satz 1 GG hergeleitet wird. Diese gebietet es dem Staat, sich schützend und fördernd vor bedrohtes Leben zu stellen, das heißt vor allem, es auch vor rechtswidrigen Übergriffen vonseiten Anderer zu bewahren.[26]

In den folgenden Jahren ergingen zahlreiche Entscheidungen des Bundesverfassungsgerichts, die die Schutzpflichtendogmatik weiter ausbauten. Diese betreffen neben dem Schwangerschaftsabbruch[27] insbesondere den Schutz vor Terrorismus[28] sowie den Schutz vor Risiken der Technik und den Umweltschutz.[29] Auch hinsichtlich des Rechts auf informationelle Selbstbestimmung ist die Schutzpflichtendimension anerkannt.[30]

---

[24] BVerfGE 1, 97 (104).

[25] BVerfGE 24, 119 (144).

[26] BVerfGE 39, 1 (42).

[27] Auf das erste Urteil folgte: BVerfGE 88, 203 (252).

[28] BVerfGE 46, 160 (164 f.) und 49, 24 (53 ff.).

[29] BVerfGE 49, 89 (142); 53, 30 (57); 56, 54 (73, 78); 77, 170 (214); 79, 174 (201 f.); BVerfG NJW 1983, 2931 (2932); NJW 1996, 651 (651); NJW 2002, 1638 (1638 f.) und NVwZ 2009, 171 (171 f.).

[30] BVerfG MMR 2007, 93, 93; NJW 2013, 3086, 3087.

Die grundrechtliche Schutzpflicht hat zudem Anerkennung durch die Rechtsprechung des Europäischen Gerichtshofs für Menschenrechte gefunden.[31] Auch hinsichtlich des Rechts auf Achtung des Privatlebens nach Art. 8 EMRK[32] und hinsichtlich Art. 10 EMRK[33] ist die Schutzpflichtendimension bestätigt. Ebenso erwachsen aus der Europäischen Grundrechte-Charta Schutzpflichten, wie Art. 51 GR-Ch belegt.[34]

III. Entstehen der Schutzpflicht

Voraussetzung für das Bestehen einer Schutzpflicht im konkreten Fall ist zunächst das Vorliegen einer Gefährdung eines grundrechtlich geschützten Interesses. Diese muss noch nicht die Intensität eines Eingriffs erreicht haben.[35] Hinreichend, aber auch erforderlich, ist eine Gefährdung, da gerade präventives Handeln des Staates in Rede steht.[36] Als Ansatzpunkt zur Bestimmung, wann die Gefährdung ausreichend groß ist, um eine Schutzpflicht entstehen zu lassen, erscheint es sinnvoll, auf den polizei- und sicherheitsrechtlichen Gefahrenbegriff zurückzugreifen. Das Polizei- und Sicherheitsrecht dient zu großen Teilen der Verwirklichung der Schutzpflicht gegen Übergriffe Dritter, sodass ein Gleichlauf der Gefährdungsanforderungen sachgemäß erscheint.[37] Demnach liegt eine suffiziente Gefährdung vor, wenn eine Sachlage oder ein Verhalten bei ungehindertem Ablauf des objektiv zu erwartenden Geschehens mit Wahrscheinlichkeit ein geschütztes Rechtsgut schädigen wird.[38]

---

[31] EGMR, Nr. 1474/62, Urt. v. 23.7.1968 (Belgischer Sprachenfall v. Belgien); weiterführend dazu: *Dröge*, Positive Verpflichtungen der Staaten in der Europäischen Menschenrechtskonvention, 2003; *Klein*, Das Untermaßverbot, JuS 2006, 960, 964 f; *Krieger*, Positive Verpflichtungen unter der EMRK, ZaöRV 2014, 187 ff.; *Mowbray*, The Development of Positive Obligations under the European Convention on Human Rights by the European Court of Human Rights, 2004; *Streuer*, Die positiven Verpflichtungen des Staates, 2003; *Tian*, Objektive Grundrechtsfunktionen im Vergleich, 2012 und *Xenos*, The Positive Obligations of the State under the European Convention of Human Rights, 2012.

[32] EGMR, Nr. 20837/92, Urt. v. 25.2.1997, Rn. 95 (Z. v. Finland) und Nr. 22009/93, Urt. v. 27.8.1997, Rn. 41 (M.S. v. Schweden); *Uerpmann-Wittzack/Jankowska-Gilberg*, Die Europäische Menschenrechtskonvention als Ordnungsrahmen für das Internet, MMR 2008, 83, 88 f.

[33] *Mayer-Ladewig*, EMRK, 2011, Art. 10, Rn. 9.

[34] Vgl. *Streinz/Michl*, Die Drittwirkung des europäischen Datenschutzgrundrechts (Art. 8 GRCh) im deutschen Privatrecht, EuZW 2011, 384, 385.

[35] Da Private nicht an Grundrechte gebunden sind, können sie in diese auch nicht eingreifen. In entsprechender Anwendung der Eingriffsdogmatik wird daher untersucht, ob der private Übergriff einen Eingriff darstellen würde oder die Gefahr eines Eingriffs bestünde, wenn die Beeinträchtigung von staatlicher Seite ausginge.

[36] *Krings*, Grund und Grenzen grundrechtlicher Schutzansprüche, 2003, 227 f.

[37] So auch: *Krings*, Grund und Grenzen grundrechtlicher Schutzansprüche, 2003, 229 ff.

[38] So der allgemein akzeptierte Gefahrenbegriff, beispielsweise in: BVerwGE 45, 51 (57); *Erichsen*, Grundrechtliche Schutzpflichten in der Rechtsprechung des Bundesverfassungsgerichts, JURA 1997, 85, 87.

Notwendig ist auch die Schutzbedürftigkeit der jeweiligen Grundrechtsträger, da dem Staat nicht die Verantwortung für jede Störung privater Rechtsbeziehungen obliegen kann.[39] Soweit ein angemessenes Schutzniveau durch private Eigenvorsorge realisiert werden kann, besteht für weitergehende staatliche Interventionen kein Anlass.[40] Eine Schutzpflicht entsteht nur, wenn die Bürger nicht in eigener Verantwortung für ihre Sicherheit sorgen können und ihnen nicht zuzumuten ist, ihre Rechte selbst zu verteidigen und notfalls die Gerichte anzurufen.[41]

IV. Umsetzung der Schutzpflicht

Besteht eine Schutzpflicht, ist danach zu fragen, welches Schutzniveau der Staat herbeiführen muss. Anerkannt ist dabei, dass mit der objektiv-rechtlichen Schutzpflicht ein subjektiver Anspruch der Grundrechtsträger auf Schutz korrespondiert.[42]

Anders als bei Eingriffskonstellationen, in denen das Übermaßverbot maßgeblich für die Bestimmung der zulässigen Eingriffsintensität ist, gilt in Schutzpflichtenkonstellationen das Untermaßverbot.[43] Dieses ist verletzt, wenn der Staat untätig geblieben ist oder die getroffenen Schutzmaßnahmen evident unzureichend, also nicht angemessen und/oder nicht wirksam sind.[44] Das Grundgesetz verlangt demnach jedenfalls ein Mindestmaß an Schutz: Dem Gesetzgeber steht es aber grundsätzlich frei, ein höheres Schutzniveau zu ergreifen.

Belasten Schutzmaßnahmen Dritte, liegt hinsichtlich deren Rechten ein Grundrechtseingriff vor, zu dessen Rechtfertigung das Übermaßverbot zu beachten ist.[45] Aus dem Untermaßverbot hinsichtlich der Schutzpflicht kann sich daher nie eine

---

[39] So auch: *Gramm*, Rechtsfragen der staatlichen AIDS-Aufklärung, NJW 1989, 2917, 2923; *Hermes*, Das Grundrecht auf Schutz von Leben und Gesundheit, 1987, 245 f.; *Littwin*, Grundrechtsschutz gegen sich selbst, 1993, 187 und *Mayer*, Untermaß, Übermaß und Wesensgehaltgarantie, 2005, 58.

[40] *Trute*, Verfassungsrechtliche Grundlagen, in: Roßnagel (Hrsg.), Handbuch Datenschutzrecht, 2003, 156, 181, Rn. 51.

[41] *Isensee*, Das Grundrecht als Abwehrrecht und als staatliche Schutzpflicht, in: Isensee/Kirchhof (Hrsg.), Handbuch des Staatsrechts der Bundesrepublik Deutschland X, 2012, 413, 543, Rn. 271.

[42] *Isensee*, Das Grundrecht als Abwehrrecht und als staatliche Schutzpflicht, in: Isensee/Kirchhof (Hrsg.), Handbuch des Staatsrechts der Bundesrepublik Deutschland X, 2012, 413, 565 ff., Rn. 321 ff. m. w. N. und *Schliesky/Hoffmann/Luch u. a.*, Schutzpflichten und Drittwirkung im Internet, 2014, 108 ff. m. w. N.

[43] St. Rspr., seit: BVerfGE 88, 203 (254 ff.), ursprünglich geprägt durch: *Canaris*, Grundrechte und Privatrecht, 184 AcP (1984), 201, 228; *ders.*, Grundrechtswirkungen und Verhältnismäßigkeitsprinzip in der richterlichen Anwendung und Fortbildung des Privatrechts, JuS 1989, 161, 163 f.; ausführlich: *Mayer*, Untermaß, Übermaß und Wesensgehaltgarantie, 2005, 63 ff.

[44] BVerfGE 77, 170 (215); 88, 203 (254); 92, 26 (46); 117, 202 (227); vgl.: BVerfGE 114, 73 (89 ff.).

[45] In diesem Sinne wird zurecht darauf hingewiesen, dass bei der Erfüllung von Schutzpflichten eine Abwägung zwischen den bedrohten Rechtsgütern der zu Schützenden und den Rechtsgütern der durch die Schutzmaßnahme betroffenen Dritten stattzufinden hat: *Jeand'Heur*, Grundrechte im Spannungsverhältnis zwischen subjektiven Freiheitsgarantien und objektiven Grundsatznormen, JZ 1995, 161, 163 f.

Pflicht zum Ergreifen von Maßnahmen ergeben, die nach Abwägung aller Interessen gegen das Übermaßverbot hinsichtlich der Rechte Dritter verstoßen und somit einen ungerechtfertigten Eingriff darstellen würden.[46] Die Kritik, dem Untermaßverbot käme „keine eigenständige Qualität" zu, da bereits „aus der Annahme der Schutzpflicht als solche […] das Gebot der Pflichterfüllung im Sinne effektiven Schutzes, das angeblich Inhalt des Untermaßverbots" sei, folge, ist unberechtigt.[47] Ihr ist entgegenzuhalten, dass dem Staat regelmäßig sehr wohl ein Spielraum bleibt zwischen dem Schutz, den er mindestens zu gewährleisten hat, um das Untermaßverbot hinsichtlich der Grundrechte der zu Schützenden zu wahren und dem Schutz, den er maximal ergreifen darf, um nicht das Übermaßverbot hinsichtlich der Grundrechte Dritter zu verletzten.

Anknüpfungspunkt der Schutzpflicht ist ein Nicht-Handeln, dieses ist naturgemäß unspezifisch.[48] Die Verfassung schreibt den Grundrechtsschutz lediglich als Ziel vor, nicht jedoch seine genaue Ausgestaltung.[49] Diese liegt nach dem Grundsatz der Gewaltenteilung und dem Demokratieprinzip beim Gesetzgeber.[50] Den staatlichen Organen kommt bei der Erfüllung der Schutzpflicht ein weiter Gestaltungsspielraum zu.[51] Der Gestaltungsspielraum bezieht sich sowohl auf die Form des Schutzes als auch auf das angestrebte Schutzniveau.[52] Mitunter ist sogar von einem weiten Einschätzungs-, Wertungs- und Gestaltungsbereich die Rede.[53] An einer konturscharfen Abgrenzung dieser Bereiche fehlt es. Zuweilen wird der Einschätzungsspielraum mit dem Entschließungsermessen der Verwaltungsbehörde verglichen, wogegen der Gestaltungsspielraum dem Auswahlermessen der Verwaltungsbehörde ähnle.[54] Die vorgeschlagene Differenzierung überzeugt zwar dogmatisch, erübrigt sich jedoch, solange der Einschätzungs- und der Gestaltungsspielraum gleichberechtigt nebeneinander stehen und vonseiten des Gesetzgebers oder des Bundesverfassungsgerichts keine rechtliche Differenzierung vorgenommen wird.

Bei der Erfüllung der Schutzpflicht in Rechnung zu stellen sind jedenfalls die Eigenart des in Rede stehenden Sachbereichs, die Möglichkeiten, sich über zukünftige Entwicklungen ein hinreichend sicheres Urteil bilden zu können und die Be-

---

[46] Vgl.: *Brüning*, Voraussetzungen und Inhalt eines grundrechtlichen Schutzanspruchs, JuS 2000, 955, 958; *Mayer*, Untermaß, Übermaß und Wesensgehaltgarantie, 2005, 59; zur Anwendung des Verhältnismäßigkeitsgrundsatzes in der Schutzpflichtendogmatik: *Cremer*, Die Verhältnismäßigkeitsprüfung bei der grundrechtlichen Schutzpflicht, DÖV 2008, 102, 103 ff.

[47] So aber: *Hain*, Der Gesetzgeber in der Klemme zwischen Übermaß- und Untermaßverbot?, DVBl. 1993, 982, 983.

[48] *Wahl/Masing*, Schutz durch Eingriff, JZ 1990, 553, 558.

[49] BVerfGE 88, 203 (254).

[50] BVerfGE 56, 51 (81).

[51] BVerfGE 77, 170 (215).

[52] *Krings*, Grund und Grenzen grundrechtlicher Schutzansprüche, 2003, 271.

[53] BVerfGE 77, 170 (214 f.); 79, 174 (202); 88, 203 (262) und 96, 56 (64).

[54] *Rupp*, Die grundrechtliche Schutzpflicht des Staates für das Recht auf informationelle Selbstbestimmung im Pressesektor, 2013, 54 ff.

deutung der betroffenen Rechtsgüter.[55] Die Schutzpflicht muss um so ernster genommen werden, je höher der Rang des bedrohten Rechtsgutes innerhalb der Wertordnung des Grundgesetzes anzusetzen ist.[56] Zu berücksichtigen sind weiter die Wahrscheinlichkeit der Gefahrenverwirklichung und die Intensität der Gefahr im Falle ihres Eintritts.[57]

Der Grundsatz der Subsidiarität staatlichen Schutzes wirkt sich nicht nur auf das Entstehen der Schutzpflicht,[58] sondern auch auf deren Umfang aus.[59] Damit dient dieser Grundsatz nicht nur der Selbstbestimmung der zu Schützenden, sondern auch den möglicherweise berührten Grundrechten störender Dritter. Zudem ist die Schutzpflicht als dynamisch zu betrachten, da aus ihr eine Korrektur- und Nachbesserungspflicht erwächst.[60] Um diese erfüllen zu können, muss sich der Gesetzgeber in angemessenen zeitlichen Abständen in geeigneter Weise vergewissern, ob das Gesetz die erwarteten Schutzwirkungen tatsächlich entfaltet oder ob sich Mängel des Konzepts oder seiner praktischen Durchführung offenbaren, die eine Verletzung des Untermaßverbots begründen.[61]

Eine verfassungsrechtliche Pflicht zum Ergreifen einer konkreten Maßnahme ist nur denkbar, wenn das Untermaßverbot ausschließlich eine einzige Handlungsvariante verbleiben lässt.[62] Für gewöhnlich wird jedoch angesichts der Komplexität der zu regelnden Sachverhalte eine Bandbreite an zulässigen Varianten bestehen.

Auch hinsichtlich der Verhinderung der Gefahren, die durch informationelle Preisgabe entstehen können, hat der Staat daher grundsätzlich die Wahl aus den unter Kapitel 4 dargestellten Maßnahmen, solange die ergriffene Maßnahme nicht evident unzureichenden Schutz bietet.

V. Pflicht zum Schutz selbstbestimmt Preisgebender

Eine Schutzpflicht zur Verhinderung informationeller Preisgabe entsteht also nach Interessenabwägung, wenn

– Beeinträchtigungen grundrechtlich geschützter Interessen durch privates Verhalten vorliegen und
– die betroffenen Grundrechtsträger schutzbedürftig sind.

Zu ihrer Umsetzung gilt dann das Untermaßverbot. Nachfolgend wird zunächst untersucht, ob diese Voraussetzungen gegeben sind hinsichtlich einer Pflicht zur Ver-

---

55 BVerfGE 50, 290 (333); 77, 170 (215) und 88, 203 (262).

56 BVerfGE 39, 1 (42).

57 *Isensee*, Das Grundrecht auf Sicherheit, 1983, 37 und *Rupp*, Die grundrechtliche Schutzpflicht des Staates für das Recht auf informationelle Selbstbestimmung im Pressesektor, 2013, 56.

58 Zur Schutzbedürftigkeit der Grundrechtsträger als Voraussetzung für das Entstehen der Schutzpflicht: siehe oben Kapitel 5,A.III.

59 *Hermes*, Das Grundrecht auf Schutz von Leben und Gesundheit, 1987, 245.

60 BVerfGE 88, 203 (309).

61 BVerfGE 88, 203 (310).

62 BVerfGE 77, 170 (215).

hinderung informationeller Preisgabe zum Schutz der selbstbestimmt Preisgebenden.

Ein Verhalten der Grundrechtsträger kann ebenso ihre grundrechtlich geschützten Interessen berühren wie ein Verhalten Dritter. Dabei sind die Konstellation, in der die Grundrechtsträger den schädigenden Erfolg selbst wollen und diejenige, in der sie die Handlung wollen und den schädigenden Erfolg in Kauf nehmen, gleichzusetzen.[63] In beiden Situationen resultiert der möglicherweise eintretende schädigende Erfolg aus der eigenen Kosten-Nutzen-Abwägung der Grundrechtsträger.

Informationelle Preisgabe kann Interessen beeinträchtigen, die durch die Informationsfreiheit und das Recht auf informationelle Selbstbestimmung der Preisgebenden geschützt werden, sodass die erste Voraussetzung für das Entstehen einer Schutzpflicht erfüllt ist. Die selbstbestimmt Preisgebenden müssten jedoch auch schutzbedürftig sein.

Bei dieser Untersuchung ist zu unterscheiden zwischen Grundrechten ohne besonderen Menschenwürdebezug, wie der Informationsfreiheit (siehe 1.), auf der einen Seite und dem eng mit der Menschenwürde verbundenen Recht auf informationelle Selbstbestimmung auf der anderen Seite (siehe 2.).

1. Pflicht zum Schutz der Informationsfreiheit

Zu klären ist zunächst, ob eine Schutzbedürftigkeit zu bejahen ist, wenn durch selbstbestimmte informationelle Preisgabe Interessen beeinträchtigt werden, die durch die Informationsfreiheit geschützt sind. Aus ihrem hohen Stellenwert ergibt sich, dass der Informationsfreiheit auch bei Bedrohungen durch Private Rechnung zu tragen ist.

Geht die Bedrohung jedoch von den Grundrechtsträgern selbst aus, ist zweifelhaft, ob von vornherein keine Schutzpflichtensituation vorliegt. *Isensee* lehnt diese ab, da es bereits an der Tatbestandsvoraussetzung des „privaten Eingriff[s]“ fehle. Eine Gleichstellung von Grundrechtsbeeinträchtigungen durch Dritte und durch die Grundrechtsträger selbst sei verfehlt.[64]

Vorzugswürdig erscheint es jedoch, auch bei Beeinträchtigungen durch die Grundrechtsträger selbst grundsätzlich Schutzpflichten zuzulassen[65] und das Entstehen der Schutzpflicht im konkreten Fall – wie auch in Dreieckskonstellationen – von der Schutzbedürftigkeit der Betroffenen abhängig zu machen. Andernfalls müsste eine Schutzpflicht konsequenterweise auch abgelehnt werden bei Gefahren,

---

[63] *Krings*, Grund und Grenzen grundrechtlicher Schutzansprüche, 2003, 209.

[64] *Isensee*, Das Grundrecht als Abwehrrecht und als staatliche Schutzpflicht, in: Isensee/Kirchhof (Hrsg.), Handbuch des Staatsrechts der Bundesrepublik Deutschland X, 2012, 413, 529 f., Rn. 244 f.

[65] Aufgrund der Schutzgutorientiertheit der Schutzpflichten muss jedenfalls grundsätzlich die Möglichkeit zum Schutz vor sich selbst bestehen: *Dietlein*, Die Lehre von den grundrechtlichen Schutzpflichten, 1992, 103: 219.

die nicht selbstbestimmte Grundrechtsträger für sich auslösen. Eine solche wird jedoch zurecht allgemein anerkannt.[66]

Es gilt die „Primärverantwortung des einzelnen“.[67] Staatlicher Schutz ist subsidiär zu Selbstschutz. Können die Grundrechtsträger die Gefährdung zumutbar selbst abwehren oder sich ihr entziehen, besteht keine Schutzpflicht.

Erst recht muss dies gelten, wenn die Gefahr überhaupt erst von den selbstbestimmt Preisgebenden ausgeht. Solange die Grenze zur Unfreiwilligkeit nicht überschritten ist, muss die Entscheidung der Nutzer respektiert werden, selbst wenn sie unvernünftig ist. Ihnen steht es jederzeit frei, von dem gefährdenden Verhalten abzulassen. Tun sie dies nicht, bedürfen sie auch keines Schutzes. Grundrechte schützen nicht gegen autonome Entscheidungen der Grundrechtsträger, sondern gewährleisten gerade deren Autonomie. Im Übrigen erschiene es zweifelhaft, staatliche Entscheidungen, gerade auch in höchstpersönlichen Angelegenheiten wie der Grundrechtsausübung, an die Stelle der Entscheidungen der Grundrechtsträger zu setzen.

Wer hingegen für eine Abwägung von Schutzpflicht und Abwehrrecht plädiert, verkennt, dass keine Schutzpflicht entsteht, wenn das gefährdende Verhalten Ausdruck freier Selbstbestimmung ist.[68] Eine generelle Pflicht zum Schutz vor sich selbst ist abzulehnen.[69] Damit besteht auch keine Pflicht zur Verhinderung selbstbestimmten Verhaltens, das sich nachteilig auf durch die Informationsfreiheit geschützte Interessen auswirken kann. Vielmehr stellt die Verhinderung selbstbestimmten Verhaltens eine reguläre „bipolare Konstellation“ dar, sodass sie der verfassungsrechtlichen Rechtfertigung bedarf.[70] In diesem Sinne führt auch das Bundesverfassungsgericht in seinem Beschluss zum Transplantationsgesetz aus: „[D]er Schutz des Menschen vor sich selbst [bedarf] als Rechtfertigungsgrund staatlicher Maßnahmen in Ansehung der durch Art. 2 Abs. 1 GG verbürgten allgemeinen Handlungsfreiheit grundsätzlich seinerseits einer verfassungsrechtlichen Rechtfertigung. Auch selbstgefährdendes Verhalten ist Ausübung grundrechtlicher Freiheit.“[71]

---

[66] In dieser Konstellation bejaht auch *Isensee* eine Schutzpflicht: *Isensee*, Das Grundrecht als Abwehrrecht und als staatliche Schutzpflicht, in: Isensee/Kirchhof (Hrsg.), Handbuch des Staatsrechts der Bundesrepublik Deutschland X, 2012, 413, 530, Rn. 246; siehe unten Kapitel 5,A.VI.

[67] *Steiger*, Entwicklungen im Grundrechtsverständnis in der Rechtsprechung des Bundesverfassungsgerichts, in: Berberich/Holl/Maaß (Hrsg.), Neue Entwicklungen im öffentlichen Recht, 1979, 255, 277.

[68] So aber: *Erichsen*, Grundrechtliche Schutzpflichten in der Rechtsprechung des Bundesverfassungsgerichts, JURA 1997, 85, 87.

[69] *Dietlein*, Die Lehre von den grundrechtlichen Schutzpflichten, 1992, 223; *Hermes*, Das Grundrecht auf Schutz von Leben und Gesundheit, 1987, 228 f.; *Klein*, Grundrechtliche Schutzpflicht des Staates, NJW 1989, 1633, 1640; *Krings*, Grund und Grenzen grundrechtlicher Schutzansprüche, 2003, 208; siehe zu den dahinterstehenden Erwägungen auch unten Kapitel 5,A.V.2.

[70] *Isensee*, Das Grundrecht als Abwehrrecht und als staatliche Schutzpflicht, in: Isensee/Kirchhof (Hrsg.), Handbuch des Staatsrechts der Bundesrepublik Deutschland X, 2012, 413, 530, Rn. 245.

[71] BVerfG NJW 1999, 3399, 3401.

So schließt *von Münch*, der sich als einer der Ersten mit der Frage der staatlichen Pflicht zum Schutz vor sich selbst auseinandersetzte, seine Untersuchung ab mit den plastischen Worten: „Die Fragestellung dieses Beitrages führte in die Sackgasse.“[72]

2. Pflicht zum Schutz des Rechts auf informationelle Selbstbestimmung

Durch informationelle Preisgabe können weiter Interessen beeinträchtigt werden, die durch das Recht auf informationelle Selbstbestimmung der Preisgebenden geschützt sind. Dieses Recht findet Gewährleistung durch Art. 2 Abs. 1 in Verbindung mit Art. 1 Abs. 1 GG und ist damit unmittelbar an die Menschenwürde angebunden. Aus diesem könnte trotz Gefährdung durch die Grundrechtsträger selbst eine besondere Schutzbedürftigkeit erwachsen, die eine von dem hinsichtlich der Informationsfreiheit gefundenen Ergebnis abweichende Beurteilung rechtfertigen könnte.

Zu klären ist, ob aus der Menschenwürde generell Pflichten zum Schutz vor sich selbst entstehen, sowie ob konkret Pflichten zum Schutz der Preisgebenden vor sich selbst folgen.

Teilweise werden grundgesetzliche Pflichten zum Schutz vor sich selbst bei Selbstgefährdung der Menschenwürde bejaht.[73] Befürworter können sich dabei insbesondere auf drei Entscheidungen stützen, die jedoch bereits zwischen 14 und 34 Jahre zurückliegen und seitdem vielfach kritisiert wurden.

Das Bundesverwaltungsgericht entschied 1981 in einem heftig umstrittenen Urteil, dass das zur Schau Stellen nackter Frauen in Peep-Shows die Menschenwürde dieser Frauen verletzt, sodass der Staat nach Art. 1 Abs. 1 Satz 2 GG zu ihrem Schutz verpflichtet ist.[74] Da die zugrunde liegenden Wertungen jedoch dem jeweils vorherrschenden Zeitgeist unterworfen sind, ist zu bezweifeln, ob diese Entscheidung heutzutage im Zeitalter der Anerkennung der Prostitution als Dienstleistung[75] nochmals in gleicher Form ergehen würde.[76] Auch beschränkt sich das Urteil aus-

---

[72] *Münch*, Grundrechtsschutz gegen sich selbst?, in: Stödter/Thieme (Hrsg.), Festschrift für Hans Peter Ipsen zum siebzigsten Geburtstag, 1977, 113, 128.

[73] Einen ausführlichen Überblick gibt *Fischer*, der sowohl eine entsprechende Schutzpflicht als auch eine Eingriffsbefugnis im Ergebnis jedoch ablehnt: *Fischer*, Die Zulässigkeit aufgedrängten staatlichen Schutzes vor Selbstschädigung, 1997, 183 ff.

[74] BVerwGE 64, 274 (277 f.); a. A. zurecht: *Fischer*, Die Zulässigkeit aufgedrängten staatlichen Schutzes vor Selbstschädigung, 1997, 253 f.; *Höfling*, Menschenwürde und gute Sitten, NJW 1983, 1582, 1582 ff.; *Krings*, Grund und Grenzen grundrechtlicher Schutzansprüche, 2003, 207 m. w. N.; *Littwin*, Grundrechtsschutz gegen sich selbst, 1993, 86 ff.; *Olshausen*, Menschenwürde im Grundgesetz, NJW 1982, 2221 ff.; *Schatzschneider*, Rechtsordnung und Prostitution, NJW 1985, 2793, 2796 f; *Teifke*, Das Prinzip Menschenwürde, 2011, 81 f.; *Vossenkuhl*, Gerechtigkeit, Paternalismus und Vertrauen, in: Fateh-Moghadam/Sellmaier/Vossenkuhl (Hrsg.), Grenzen des Paternalismus, 2010, 163, 168 und *Würkner*, Prostitution und Menschenwürdeprinzip, NVwZ 1988, 600, 600 ff.

[75] Gesetz zur Regelung der Rechtsverhältnisse der Prostituierten (ProstG) (BGBl. I, 2001, 3983).

[76] Eine provokante Erklärung für die Haltung eines amerikanischen Gerichts in einem ähnlich gelagerten Fall liefert *Judge Posner*: „The true reason I think for wanting to exclude striptease dancing from the protection of the First Amendment is […] a feeling that the proposition, ‘the First

drücklich auf den dort gegenständlichen Sachverhalt, in dem der Staat aufgrund des gewerberechtlichen Erlaubnisvorbehalts eine „unmittelbare(…) Mitverantwortung" innehatte und lässt offen, wie die Rechtslage ohne diese staatliche Beteiligung zu beurteilen wäre.[77]

Nach einer Entscheidung des Bundesverwaltungsgerichts aus dem Jahr 2001 ist das Verbot von Laserdrome-Spielen gerechtfertigt. Die Freiwilligkeit der Teilnahme sowie das gegenseitige Einvernehmen der Spieler ist rechtlich unerheblich, „weil die aus Art. 1 Abs. 1 und Art. 2 Abs. 2 Satz 1 GG herzuleitende Wertordnung der Verfassung nicht im Rahmen eines Unterhaltungsspiels zur Disposition" steht.[78] Auch hier stellt das Bundesverwaltungsgericht aber nicht auf die Menschenwürde der freiwillig teilnehmenden Personen ab, sondern auf das gesamtgesellschaftliche Interesse an der Wahrung der Menschenwürde.

Schließlich wurde 1992 hinsichtlich des Verbots des sogenannten Zwergenweitwurfs vom Verwaltungsgericht Neustadt eine Pflicht zum Schutz der Menschenwürde vor den Grundrechtsträgern selbst konstruiert. Es kommt nicht darauf an, dass sich der Betroffene freiwillig werfen lässt und die Veranstaltung nicht als entwürdigend empfindet. Vielmehr ist die Würde des Menschen ein unverfügbarer Wert, auf dessen Beachtung die Einzelnen nicht wirksam verzichten können.[79] Auch hier weist das Gericht jedoch daraufhin, dass aufgrund des gewerberechtlichen Erlaubnisvorbehalts eine „unmittelbare(…) Mitverantwortung des Staates" besteht und daher Schutz geboten ist.[80]

Der Ansatz, aus der Beeinträchtigung der Menschenwürde erwachse eine erhöhte Schutzbedürftigkeit, die selbst bei selbstbestimmter Gefährdung durch die Betroffenen gelte, erscheint jedoch bedenklich.

Amendment forbids the State of Indiana to require striptease dancers to cover their nipples,' is ridiculous. It strikes judges as ridiculous in part because most of us are either middle-aged or elderly men, in part because we tend to be snooty about popular culture, in part because as public officials we have a natural tendency to think political expression more important than artistic expression, in part because we are Americans – which means that we have been raised in a culture in which puritanism, philistinism, and promiscuity are complexly and often incongruously interwoven – and in part because like all lawyers we are formalists who believe deep down that the words in statutes and the Constitutions mean what they say, and a striptease is not a speech.", Miller v. Civil City of South Bend, 904 F.2d 1081, 1099 f. (7th Cir. 1990) (*Posner, J.* concurring).

[77] BVerwGE 64, 274 (279).

[78] BVerwGE 115, 189 (202), aufrechterhalten durch: BVerwG GewArch 2007, 247 f.; dazu: EuGH EuZW 2004, 753 ff. Die Entscheidung stößt jedoch auf Ablehnung, da es wesentliches Element der Entfaltungsfreiheit sei, selbst darüber zu entscheiden, wie sie genutzt wird: *Teifke*, Das Prinzip Menschenwürde, 2011, 83 f. Da auf die Menschenwürde nicht wirksam verzichtet werden könnte, müsse ihr Schutzbereich eng ausgelegt werden, sodass durch Laserdrome-Spiele schon kein durch die Menschenwürde geschütztes Interesse berührt werde: *Fischinger*, Der Grundrechtsverzicht, JuS 2007, 808, 811.

[79] VG Neustadt NVwZ 1993, 98, 99; ablehnend: *Schwabe*, Der Schutz des Menschen vor sich selbst, JZ 1998, 66, 70 und *Teifke*, Das Prinzip Menschenwürde, 2011, 84 ff.

[80] VG Neustadt NVwZ 1993, 98, 99.

Kritisch äußert sich zurecht das Oberverwaltungsgericht Lüneburg, wenn es anlässlich seiner Paintball-Entscheidung für die Verhinderung mittelbarer und abstrakter Menschenwürdebeeinträchtigungen durch die Grundrechtsträger selbst einen erhöhten Begründungsaufwand für staatliches Tätigwerden fordert, der über den hinausgeht, der bei Verletzungen durch den Staat oder Dritte vonnöten ist.[81] Die im Verfahren vorgetragenen Beeinträchtigungen durch Paintball-Spiele erfüllten diese Voraussetzung nicht.

Die Menschenwürde schützt die Einzelnen davor, bloßes Objekt staatlichen Handelns zu werden.[82] Dieser Schutz gewährleistet auch, dass die Menschen über sich selbst verfügen und ihr Schicksal eigenverantwortlich gestalten können.[83] Durch staatliche Festlegung eines objektiven Inhalts der Menschenwürde der sich selbst gefährdenden Individuen werden diese zum Objekt staatlichen Handelns, sodass gerade die proklamierten Schutzmaßnahmen einen Eingriff in die jeweiligen Grundrechte der Handelnden bedeuten. Die unzutreffende Darstellung des Eingriffs als Erfüllung einer postulierten Schutzpflicht kann hieran nichts ändern. Die Konstellation der „Menschenwürde als Eingriffsermächtigung“[84] ist im Rahmen der Rechtfertigung von Grundrechtseingriffen zu diskutieren, nicht jedoch als Erfüllung einer Schutzpflicht zu behandeln.

Wie sehr der aufgezwungene Schutz vor vermeintlichen Menschenwürdebeeinträchtigungen durch sich selbst zu staatlicher Bevormundung ausarten kann, zeigt sich beispielsweise, wenn auf Basis der dargestellten Überlegungen ein Menschenwürdeverstoß der Fernsehsendung Big Brother konstruiert wird. Die Autonomie der Einzelnen müsse sich immer im Rahmen der Menschenwürde bewegen, könne sie aber nicht überschreiten oder gar ersetzen.[85] Diese Annahme verkennt, dass Ausdruck der individuellen Autonomie gerade ist, sich selbstbestimmt im eigenen Umfeld zu platzieren.

Es erscheint vorzugswürdig, eine Schutzbedürftigkeit auch hinsichtlich etwaiger Menschenwürdebeeinträchtigungen abzulehnen. Das aus dieser Handhabung folgende Ergebnis ist durchaus sachgerecht: Das in Rede stehende Verhalten ist notwendigerweise Ausdruck eines Art. 1 GG nachfolgenden Grundrechts der Handelnden und kann zum Schutz anderer Interessen eingeschränkt werden. Dabei bedarf es jedoch der Interessenabwägung zwischen den kollidierenden Rechtsgütern. Fällt diese zu Lasten der Handelnden aus, ist es verfassungsrechtlich zulässig und rechts-

---

[81] OVG Lüneburg NJOZ 2010, 1997, 2001.

[82] St. Rspr., statt vieler: BVerfGE 27, 1 (6).

[83] BVerfGE 49, 286 (298).

[84] Diese treffende Bezeichnung wählt *Teifke*. Er führt weiter aus: „An dieser Stelle geht es lediglich um die Fälle, in denen die Menschenwürde als Eingriffsermächtigung fungiert, nicht um das Würdegrundrecht eines Einzelnen zu schützen, sondern um staatliche Eingriffe in Grundrechte Einzelner durch Rückgriff auf die Menschenwürde zu rechtfertigen.“: *Teifke*, Das Prinzip Menschenwürde, 2011, 80.

[85] *Hinrichs*, „Big Brother“ und die Menschenwürde, NJW 2000, 2173, 2175; dagegen richtigerweise: *Huster*, Individuelle Menschenwürde oder öffentliche Ordnung?, NJW 2000, 3477 ff.

politisch wünschenswert, die Selbstgefährdung zu verhindern. Ergibt die Interessenabwägung jedoch ein Überwiegen der Interessen der Selbstgefährdenden, besteht kein Anlass zur Intervention.

Auf die Ablehnung der Pflicht zum Schutz der Menschenwürde kommt es hier jedoch gar nicht an. Die Konstellationen der Peep-Show, der Laserdrome-Spiele und des „Zwergenweitwurfs" führen bereits tatsächlich dazu, dass Menschen von anderen Menschen physisch und in direkter, realer Konfrontation als Objekt behandelt werden. Die Diskussion um den Schutz der Menschenwürde der Betroffenen ist damit jedenfalls berechtigt.

Die Preisgabe personenbezogener Daten ist mit solchen Sachverhalten nicht vergleichbar. Zwar hat das Recht auf informationelle Selbstbestimmung einen Menschenwürdekern, doch führt eine Preisgabe von Daten im Internet maximal zu einer digitalen, nicht jedoch zu einer körperlichen und realen Verobjektivierung der Preisgebenden. Die Situation ist daher nicht mit den anderen drei vergleichbar. Auch wenn man eine Pflicht zum Schutz der Menschenwürde entgegen der hier bevorzugten Auffassung bejahen würde, müsste sich diese jedenfalls auf eindeutige Beeinträchtigungen der Menschenwürde konzentrieren. Angesichts des „Menschenwürdekerns"[86] aller Grundrechte wären sonst einer ausufernden staatlichen Bevormundung Tür und Tor geöffnet.

Zusammenfassend lässt sich sagen, dass durch informationelle Preisgabe zwar die informationelle Selbstbestimmung bedroht werden kann. Diese wird geschützt durch Art. 2 Abs. 1 in Verbindung mit Art. 1 Abs. 1 GG und hat damit einen Menschenwürdekern. Eine Bejahung einer Pflicht zum Schutz der Menschenwürdeträger vor sich selbst erscheint jedoch bedenklich, da sie die Gewährleistung der Menschenwürde in ihr Gegenteil verkehren würde. Darauf kommt es jedoch im Ergebnis nicht an, da sich eine etwaige Pflicht zum Schutz der Menschenwürde nicht auf Beeinträchtigungen von durch das Recht auf informationelle Selbstbestimmung geschützten Interessen erstreckt.

Überzeugend formuliert *Kutscha*, die grundsätzliche Anerkennung von Schutzpflichten dürfe „freilich nicht als verfassungsrechtliche Einladung zur Bevormundung der Einzelnen durch den Staat missverstanden werden. Informationelle Selbstbestimmung kann eben auch darin bestehen, sein Privatleben wissentlich und freiwillig gegenüber einer weltweiten Öffentlichkeit zu offenbaren".[87]

3. *Pflicht zur Sicherung der Selbstbestimmung*

Die vorangegangenen beiden Kapitel befassten sich mit dem Schutz des selbstbestimmt Preisgebenden vor sich selbst. Hier war eine Schutzpflicht abzulehnen, da

---

[86] Zur Herleitung des Menschenwürdekerns der Grundrechte m.w.N.: Maunz/Dürig-GG/*Herdgen*, 2014, Art. 1, Rn. 26f.

[87] *Kutscha*, Erster Teil, in: Kutscha/Thomé (Hrsg.), Grundrechtsschutz im Internet?, 2013, 11, 47.

die selbstbestimmte Entscheidung zur Preisgabe zu akzeptieren ist, sodass die Preisgebenden nicht schutzbedürftig sind.

Etwas anderes könnte jedoch gelten, wenn gerade die Selbstbestimmtheit der Preisgabe in Frage steht. In dieser Konstellation könnte das Hauptargument gegen das Entstehen der Schutzpflicht – der Vorrang der selbstbestimmten Entscheidung – wegfallen und eine Schutzpflicht entstehen. Diese könnte darauf zielen, die Selbstbestimmung der Nutzer hinsichtlich ihrer informationellen Preisgabe zu fördern, um einem Verlust der Selbstbestimmung vorzubeugen.

Angesichts unvorhersehbarer Folgen und schwieriger technischer Zusammenhänge ist im Internetkontext die Grenze zwischen selbstbestimmter und nicht selbstbestimmter Preisgabe fließend. Selbstbestimmung setzt nicht Freiheit von jedem sozialen oder wirtschaftlichen Druck voraus. Sie verlangt nicht nach einem Kräftegleichgewicht zwischen den Parteien. Dies mag zunächst unfair erscheinen, fehlt es einer Seite doch häufig an der Verhandlungsmacht, die Konditionen der Preisgabe zu verhandeln. In Rechtsprechung und Literatur ist daher anerkannt, dass eine grundrechtliche Schutzpflicht besteht, den Nutzern eine selbstbestimmte informationelle Preisgabe im Internet zu gewährleisten:

Das Bundesverfassungsgericht entschied in diesem Sinne (wenn auch in einem etwas anderen Kontext), dass den Einzelnen wirkungsvoller informationeller Selbstschutz ermöglicht werden muss, indem die Bedingungen geschaffen und erhalten werden, unter denen sie selbstbestimmt an Kommunikationsprozessen teilnehmen und so ihre Persönlichkeit entfalten können.[88]

Auch in der Literatur ist anerkannt, dass es eines gesetzlichen Rahmens bedarf, der den Grundrechtsträgern die Gelegenheit für eine differenzierte Selbstbestimmung über die Aufgabe ihrer Privatheit eröffnet.[89] Den Bürgern steht ein Recht auf Schaffung und Erhaltung der Bedingungen zu, unter denen eine freiheitliche Darstellung der eigenen Persönlichkeit möglich ist.[90]

Der Staat muss die Akteure befähigen, selbstbestimmt und eigenverantwortlich einen Beitrag zur Sicherheit der Informationstechnik zu leisten.[91] Es besteht daher die staatliche Infrastrukturverantwortung, den Einzelnen effektiven Selbstschutz zu ermöglichen.[92]

---

[88] BVerfG MMR 2007, 93, 93.

[89] *Kutscha*, Erster Teil, in: Kutscha/Thomé (Hrsg.), Grundrechtsschutz im Internet?, 2013, 11, 47 und *Masing*, Herausforderungen des Datenschutzes, NJW 2012, 2305, 2308.

[90] *Trute*, Verfassungsrechtliche Grundlagen, in: Roßnagel (Hrsg.), Handbuch Datenschutzrecht, 2003, 156, 170, Rn. 22, 24.

[91] Vgl.: *Britz*, Informationelle Selbstbestimmung zwischen rechtswissenschaftlicher Grundsatzkritik und Beharren des Bundesverfassungsgerichts, in: Hoffmann-Riem (Hrsg.), Offene Rechtswissenschaft, 2010, 561, 592; *Heckmann*, Digitales Dilemma, 2012 und *Roßnagel*, Konzepte des Selbstdatenschutzes, in: ders. (Hrsg.), Handbuch Datenschutzrecht, 2003, 325, 335.

[92] *Roßnagel/Pfitzmann/Garstka*, Modernisierung des Datenschutzrechts, 2001, 150 ff.; *dies.*, Modernisierung des Datenschutzrechts, DuD 2001, 253, 261; siehe allgemein: *Zoche/Ammicht-Quinn/Lamla u. a.* (Hrsg.), White Paper Selbstdatenschutz, 2014.

Staatlicher Schutz muss sich auf Maßnahmen beschränken, die die Selbstbestimmung fördern, sodass die Einzelnen nicht in die Unfreiwilligkeit abgleiten. Der Staat muss dabei darauf hinwirken, dass sich die Nutzer selbst effektiv schützen können oder sich jedenfalls aus eigenem Antrieb der staatlichen Schutzmechanismen bedienen. Gleichzeitig gilt jedoch: Ultra posse nemo obligatur – der Staat muss die Selbstbestimmung der Nutzer nur in dem Rahmen fördern, in dem ihm dies auch möglich ist.[93]

Zur Erfüllung der Schutzpflicht kommt dem Staat ein weiter Gestaltungsspielraum zu. Bei der Auswahl aus den zur Verfügung stehenden Mitteln – dem erzwungenen Schutz, der Unterstützung informationellen Selbstschutzes und den Entscheidungsarchitekturen – ist das Untermaßverbot[94] zu beachten.

Erzwungener Schutz scheidet als mögliches Mittel aus, da er Selbstbestimmung verhindert und somit unwirksam zur Sicherung von Selbstbestimmung ist.

Die Unterstützung informationellen Selbstschutzes sowie Maßnahmen der Entscheidungsarchitektur hingegen können wirkungsvollen Schutz bieten. Beide Maßnahmen sind auch nicht evident unzureichend. Jedoch belassen Entscheidungsarchitekturen den Preisgebenden weniger Selbstbestimmung, als es die bloße Unterstützung informationellen Selbstschutzes tut, weil durch Vorgaben der Architektur die Einzelnen gerade in eine Richtung „geschubst" werden, die sie sich nicht (primär) selbst aussuchen. Angesichts der Primärverantwortung der Preisgebenden ist daher soweit wie möglich von Entscheidungsarchitekturen abzusehen und der Schwerpunkt auf die Unterstützung informationellen Selbstschutzes zu legen. Durch diesen wird den Grundrechtsträgern ermöglicht, Gefahren aus eigener Entscheidung nicht auf sich zu nehmen beziehungsweise sich selbst zu schützen.

Im Folgenden seien zur Veranschaulichung einige einfachrechtliche Beispiele der Unterstützung informationellen Selbstschutzes herausgegriffen.

Zentrales Instrument des deutschen (und europäischen) informationellen Selbstschutzes ist das datenschutzrechtliche Verbotsprinzip (Art. 7 DSRL, § 4 Abs. 1 BDSG, § 12 Abs. 1 TMG). Das deutsche Datenschutzrecht erlaubt, anders als das US-amerikanische Recht, die Erhebung, Verarbeitung und Nutzung personenbezogener Daten nur, wenn eine Befugnis durch Rechtsvorschrift gegeben ist oder eine Einwilligung vorliegt. Zwar kommt dem datenschutzrechtlichen Verbotsprinzip eine Art Zwitter-Stellung zwischen der Unterstützung informationellen Selbstschutzes und den Entscheidungsarchitekturen zu, da es der Tendenz der Nutzer zum Belassen von Voreinstellungen folgt und nicht gesetzlich autorisierte Preisgabe verhindert, solange die Nutzer keine Einwilligung erteilen. Doch bezweckt es nicht, die Nutzer an bestimmter informationeller Preisgabe zu hindern. Vielmehr wird

[93] *Schliesky/Hoffmann/Luch u. a.*, Schutzpflichten und Drittwirkung im Internet, 2014, 180; allgemein zum „Vorbehalt des Möglichen": *Isensee*, Das Grundrecht als Abwehrrecht und als staatliche Schutzpflicht, in: Isensee/Kirchhof (Hrsg.), Handbuch des Staatsrechts der Bundesrepublik Deutschland X, 2012, 413, 544 f., Rn. 274 ff.

[94] St. Rspr., seit: BVerfGE 88, 203 (254 ff.); siehe oben Kapitel 5,A.IV.

überhaupt erst die Grundlage für eine Entscheidung über die Preisgabe gelegt, soweit keine gesetzliche Grundlage vorliegt. Ohne das datenschutzrechtliche Verbotsprinzip wäre es den Nutzern regelmäßig gänzlich verwehrt, auf die Erhebung und Nutzung ihrer Daten ex ante Einfluss zu nehmen. Daher ist es der Kategorie der Unterstützung informationellen Selbstschutzes zuzuordnen.

Davon abgesehen liegt der Schwerpunkt der Unterstützung informationellen Selbstschutzes derzeit noch auf dem Konzept der Unterrichtung der Preisgebenden:[95]

Die Fälle der Befugnis durch Rechtsvorschrift gehen regelmäßig einher mit entsprechenden Unterrichtungs- und Benachrichtigungsvorschriften, wie § 4 Abs. 3 BDSG (Unterrichtungspflicht bei der Erhebung personenbezogener Daten bei den Betroffenen) und § 33 Abs. 1 BDSG (Benachrichtigungspflicht bei der Speicherung personenbezogener Daten ohne Kenntnis der Betroffenen). Über § 12 Abs. 3 TMG finden diese Vorschriften auch Anwendung auf Anbieter von Telemedien. Von diesen zu beachten ist auch die Unterrichtungsvorschrift des § 13 Abs. 1 TMG.

Noch größere Relevanz kommt den Unterrichtungsvorschriften bei der Einwilligung zu. Nach Art. 2 lit. h DSRL ist die Einwilligung eine Willensbekundung, die ohne Zwang, für den konkreten Fall und in Kenntnis der Sachlage erfolgt und mit der die Betroffenen akzeptieren, dass sie betreffende personenbezogene Daten verarbeitet werden. Die Umsetzung ins deutsche Recht erfolgt durch § 4a Abs. 1 BDSG, der die näheren Voraussetzungen der datenschutzrechtlichen Einwilligung bestimmt. Bedingung ist neben der Freiwilligkeit der Entscheidung (§ 4a Abs. 1 BDSG: „freie Entscheidung“; Art. 2 lit. h DSRL: „ohne Zwang“) die Informiertheit der Einwilligenden (Art. 2 lit. h DSRL: „in Kenntnis der Sachlage“). Letzterer Voraussetzung trägt § 4a Abs. 1 Satz 2 BDSG Rechnung, der vorsieht, dass die Einwilligenden auf den vorgesehenen Zweck der Erhebung, Verarbeitung oder Nutzung sowie, soweit nach den Umständen des Einzelfalles erforderlich oder auf Verlangen, auf die Folgen der Verweigerung der Einwilligung hinzuweisen sind.

Weiter zu nennen sind Regelungen, die unabhängig vom Willen der Preisgebenden die Modalitäten der Datenpreisgabe festlegen, wie beispielsweise § 4a Abs. 1 Satz 2–4 BDSG (Hinweis-/Schriftform-/Hervorhebungspflicht)[96] und § 4a Abs. 3 BDSG (ausdrücklicher Bezug).

Zur Unterrichtung hinzu treten die dargestellten ergänzenden Konzepte. Ein Beispiel für alternative Unterrichtungsmethoden[97] stellt die Liste der Datenschutz-Symbole dar, die die LIBE-Fassung des Entwurfs der EU-Datenschutz-Grundverordnung in Anhang 1 (zu Art. 13a) enthält.[98]

---

[95] Siehe oben Kapitel 4,B.I.

[96] Im Bereich des Telemediengesetzes geltend nach § 13 Abs. 2 TMG gelockerte Anforderungen, ebenso im Bereich des Telekommunikationsgesetzes gemäß § 94 TKG.

[97] Siehe oben Kapitel 4,B.II.

[98] Die vorgeschlagenen Symbole sind allerdings nicht unbedingt intuitiv verständlich.

Als Beispiel für technischen Selbstschutz[99] dienen kann § 13 Abs. 6 Satz 1 TMG, nach dem die Diensteanbieter die Nutzung von Telemedien und ihre Bezahlung anonym oder unter Pseudonym zu ermöglichen haben, soweit dies technisch möglich und zumutbar ist. Auch das Konzept des Datenschutzes als Bildungsauftrag findet verstärkten Anklang.[100]

Auf Entscheidungsarchitekturen wird im Bereich des Datenschutzrechts durch den Staat derzeit hingegen noch nicht in signifikanter Weise zurückgegriffen, insbesondere gibt es noch keine verpflichtenden Privatheitsvoreinstellungen für Internetanwendungen. Eine Pflicht zu Privacy by Default enthält hingegen Art. 23 Abs. 2 EU-DS-GVO-E. Ob, wann und in welcher Gestalt die EU-Datenschutz-Grundverordnung in Kraft tritt, ist jedoch noch unklar.

VI. Pflicht zum Schutz nicht selbstbestimmt Preisgebender

Weiter könnte eine Pflicht zum Schutz Derjenigen bestehen, die nicht selbstbestimmt ihre informationelle Privatheit im Internet preisgeben und denen auch durch Aufklärung nicht zur Selbstbestimmtheit verholfen werden könnte.

Aus der informationellen Preisgabe können Bedrohungen für Interessen erwachsen, die durch das Recht auf informationelle Selbstbestimmung sowie die Informationsfreiheit der Preisgebenden geschützt werden.[101] Eine Schutzpflicht entsteht, wenn die nicht selbstbestimmt Preisgebenden zudem schutzbedürftig sind, also das gefährdende Verhalten nicht Ausdruck ihrer freien Selbstbestimmung ist.[102] Sinnvollerweise kann unterteilt werden in die Konstellationen der fehlenden Einsichtsfähigkeit sowie der fehlenden Wahlmöglichkeit.

Fehlende Einsichtsfähigkeit kann vorliegen bei psychisch Kranken und geistig Behinderten sowie bei Minderjährigen (abgestuft je nach Alter).[103]

In seinem Urteil zum Baden-Württembergischen Unterbringungsgesetz führt das Bundesverfassungsgericht aus: „Bei psychischer Erkrankung wird die Fähigkeit zur Selbstbestimmung häufig erheblich beeinträchtigt sein. In solchen Fällen ist dem Staat fürsorgerisches Eingreifen auch dort erlaubt, wo beim Gesunden Halt geboten ist. […] Zumal unter der Geltung des Sozialstaatsgedankens (Art. 20 Abs. 1, 28 GG) ist kein Grund ersichtlich, der es hindern könnte, die Fürsorge für die Bürger, die

---

[99] Siehe oben Kapitel 4,B.III.

[100] Siehe oben Kapitel 4,B.IV; *Wagner*, Datenschutz als Bildungsauftrag, DuD 2012, 83, 86 f. und *ders.*, Datenschutz als Bildungsaufgabe, in: Schmidt/Weichert (Hrsg.), Datenschutz, 2012, 88 ff.

[101] Siehe oben Kapitel 3,B.I.

[102] Vgl.: BVerfGE 58, 208 (225); 81, 242 (255); *Dietlein*, Die Lehre von den grundrechtlichen Schutzpflichten, 1992, 220; *Hillgruber*, Der Schutz des Menschen vor sich selbst, 1992, 121 ff.; *Klein*, Grundrechtliche Schutzpflicht des Staates, NJW 1989, 1633, 1640.

[103] BVerfGE 58, 208 (224 ff.); BVerwG NJW 1989, 2960 f.; BayVGH NJW 1989, 1790, 1790 f.; *Hillgruber*, Der Schutz des Menschen vor sich selbst, 1992, 69 f. Auch *Mill* macht eine Ausnahme bei Menschen mit nicht „völlig ausgereiften Fähigkeiten“: *Mill*, Über die Freiheit, 2010 (Original: 1859), 19.

hilfsbedürftig sind, weil sie psychisch krank sind, als staatliche Aufgabe auszugestalten." Entsprechend ermöglicht das Recht es, „den Willen des psychisch Kranken durch die bessere Einsicht des für ihn Verantwortlichen zu ersetzen".[104]

Weiter sind angesichts des sozialen Drucks zur Internetnutzung gerade Minderjährige einem erhöhten Bedrohungspotenzial ausgesetzt. Die Vielzahl der Möglichkeiten kann sie leicht zu nicht selbstbestimmter informationeller Preisgabe bestimmen, deren Konsequenzen sie nicht überblicken können.[105]

Mangelt es den Preisgebenden aufgrund Krankheit, Behinderung oder Minderjährigkeit an Einsichtsfähigkeit, ist eine etwaige Preisgabe nicht Ausdruck ihres selbstbestimmten Handelns, sodass der Staat zum Schutz aufgerufen ist.

An Wahlmöglichkeiten fehlt es, wenn die Auswahl von Vorneherein durch faktische Zwänge (also Machtdisparität oder das Angewiesensein auf ein bestimmtes Produkt) oder unverschuldete mangelnde Informiertheit auf sehr wenige Optionen oder nur eine limitiert ist.[106]

Klassisches Beispiel für faktische Zwänge ist die fehlende Vertragsfreiheit. Obwohl das Bundesverfassungsgericht teilweise den Begriff Schutzpflicht nicht ausdrücklich verwendet, gehört eine Reihe von Entscheidungen aus dem Vertrags- und Arbeitsrecht in diese Kategorie.[107] Auch wenn Grundrechtsträger selbst Vertragsverhältnisse eingehen und sich damit in Gefahr begeben, können Situationen bestehen, in denen aufgrund eines Machtungleichgewichts die Vertragsparität gestört ist. Privatautonomie setzt voraus, dass die Bedingungen der Selbstbestimmung der Einzelnen auch tatsächlich gegeben sind.[108] Da nicht nur das „Recht des Stärkeren"[109] gelten darf, kann ein staatliches Einschreiten erforderlich sein. An Vertragsfreiheit fehlt es, wenn kein Mindestmaß an effektiver Unabhängigkeit gegenüber dem Anderen vorliegt, um den eigenen Willen zur Geltung zu bringen und nicht unausweichlich darauf angewiesen zu sein, sich dem Vertragsdiktat des Anderen zu fügen.[110] Eine solche Situation ist gegeben, wenn einer der Vertragsteile ein so starkes Übergewicht hat, dass vertragliche Regelungen faktisch einseitig gesetzt wer-

---

[104] BVerfGE 58, 208 (225).

[105] Hierzu ausführlich: *Jandt/Roßnagel*, Social Networks für Kinder und Jugendliche, MMR 2011, 637 ff.; *Schenk/Neumann/Reinmann u. a.* (Hrsg.), Digitale Privatsphäre, 2012; Europäische Strategie für ein besseres Internet für Kinder vom 2.5.2012 und *Europäischer Datenschutzbeauftragter*, Stellungnahme 17.7.2012.

[106] Vorrangig muss versucht werden, Wahlmöglichkeiten durch die im vorstehenden Abschnitt beschriebenen Maßnahmen zur Sicherung der Selbstbestimmung zu erreichen. Erst, wenn dies nicht möglich ist, ist tatsächlich vom in diesem Abschnitt behandelten Fehlen der Selbstbestimmung auszugehen.

[107] BVerfGE 81, 242 (255 f.); 89, 214 (232); 97, 169 (176 f.); 103, 89 (101 f.) und 114, 1 (34).

[108] BVerfGE 81, 242 (254 f.); 103, 89 (100); 114, 1 (34); vgl.: *Globig*, Zulässigkeit der Erhebung, Verarbeitung und Nutzung im öffentlichen Bereich, in: Roßnagel (Hrsg.), Handbuch Datenschutzrecht, 2003, 627, 643, Rn. 41.

[109] BVerfGE 89, 214 (232).

[110] *Isensee*, Privatautonomie, in: Isensee/Kirchhof (Hrsg.), Handbuch des Staatsrechts der Bundesrepublik Deutschland VII, 2009, 207 ff., Rn. 24.

den können.[111] Die Grundrechtsposition der einen wird dann den Interessen der anderen Vertragspartei in einer Weise untergeordnet, dass in Anbetracht der Bedeutung und Tragweite des betroffenen Grundrechts von einem angemessenen Ausgleich nicht mehr gesprochen werden kann.[112] Insbesondere am Beispiel dieser Fallgruppe wird das Zusammenspiel von mittelbarer Drittwirkung und Schutzpflicht deutlich: Grundrechte verpflichten den Staat zum Schutz der Grundrechtsträger gegen andere Private durch Schaffung einer Rechtsordnung, in der tatsächliche Privatautonomie herrscht. Bei Auslegung und Anwendung der Rechtsnormen entfalten die in Rede stehenden Grundrechte dann mittelbare Drittwirkung.

Faktische Zwänge führen zur Unwirksamkeit der Einwilligung, wenn die Einwilligenden so essenziell auf die mit der Einwilligung zusammenhängende Leistung angewiesen sind, dass ihnen ein Verzicht darauf nicht zuzumuten ist.[113] Nach der Payback-Entscheidung des Bundesgerichtshofs kann ein faktischer Zwang vorliegen, „wenn die Einwilligung in einer Situation wirtschaftlicher oder sozialer Schwäche oder Unterordnung erteilt wird“ oder wenn die Betroffenen „durch übermäßige Anreize finanzieller oder sonstiger Natur zur Preisgabe ihrer Daten verleitet“ werden.[114] Ein faktischer Zwang liegt mangels Angewiesenseins auf das Angebot beispielsweise jedoch nicht schon dann vor, wenn die Einzelnen auf die Nutzung eines großen sozialen Netzwerks nicht verzichten wollen, um sozialer Ausgrenzung vorzubeugen.

In Sonderfällen kann schließlich auch fehlende Informiertheit zu fehlender Wahlmöglichkeit führen und so eine Schutzpflicht hervorrufen. *Mill* macht hierfür eine Ausnahme von seiner sonst strengen Ablehnung des Paternalismus: „Wenn ein öffentlicher Beamter oder sonst jemand sieht, wie ein Mensch eine Brücke überschreiten will, die erwiesenermaßen unsicher ist, und keine Zeit mehr hat, ihn vor der Gefahr zu warnen, so darf er ihn – ohne seine Freiheit zu beeinträchtigen – anfassen und zurückziehen. Denn Freiheit besteht darin, zu tun, was man will, und der Betroffene will ja nicht ins Wasser fallen.“[115] Dieser Fall liegt im Ausgangspunkt so wie im Abschnitt zuvor (siehe V.3). Der entscheidende Unterschied ist aber, dass es wegen besonderer Umstände (hier die zeitliche Nähe) nicht möglich ist, den Betroffenen zu informieren und ihm so eine selbstbestimmte Entscheidung zu ermöglichen.

Fehlt es an Einsichtsfähigkeit oder Wahlmöglichkeit und somit an freier Selbstbestimmung über die Aufgabe ihrer Daten, muss der Staat die Einzelnen vor der nicht selbstbestimmten Preisgabe schützen. Der Staat muss mithin „eingrenzende Regeln“ erlassen, soweit dies zur Sicherung der Selbstbestimmung der Einzelnen not-

---

[111] BVerfGE 81, 242 (255).

[112] BVerfGE 97, 169 (176 f.).

[113] BVerfG MMR 2007, 93 (93); bekräftigt durch: BVerfG RDG 2013, 230 ff.; vgl.: *Nehf*, Shopping for Privacy Online, 1 Univ. of Illinios J. of L., Tech. and Policy (2005), 1, 4, 11.

[114] BGHZ 177, 253 (260 f.).

[115] *Mill*, Über die Freiheit, 2010 (Original: 1859), 138.

wendig ist.[116] Bei der Erfüllung dieser Schutzpflicht gilt wiederum das Untermaßverbot.[117] Auch hier hat der Staat aus den drei zur Verfügung stehenden Maßnahmekategorien auszuwählen.

Geeignet ist eine Maßnahme, wenn sie eine selbstbestimmte Entscheidung über die Preisgabe fördern beziehungsweise die nicht selbstbestimmte Preisgabe verhindern kann. Nicht selbstbestimmte Nutzer auf die Möglichkeit des informationellen Selbstschutzes zu verweisen, ist nicht wirksam und damit eine Verletzung des Untermaßverbots. Ebenso lassen Entscheidungsarchitekturen die Möglichkeit, sich für die Grundrechtsbeeinträchtigung zu entscheiden. Da eine solche Entscheidung jedoch nicht selbstbestimmt wäre, bietet auch Entscheidungsarchitektur keinen wirksamen Schutz und verletzt damit das Untermaßverbot. Da nicht selbstbestimmt Preisgebende gerade nicht zu selbstbestimmtem Handeln veranlasst werden können, ist lediglich erzwungener Schutz geeignet, entweder durch gesetzliche Verbote oder durch technische Unmöglichmachung der Preisgabe. Innerhalb der Kategorie des erzwungenen Schutzes besteht der staatliche Gestaltungsspielraum. Dabei kann auch auf verbindliche Maßnahmen zurückgegriffen werden, die (auf freiwilliger Basis) aus dem Bereich der Entscheidungsarchitekturen bekannt sind. Beispielsweise wird vorgeschlagen, zum Schutz von Minderjährigen zunächst nicht veränderbare altersgerechte Standard-Datenschutzeinstellungen einzuführen.[118] Solange ein Abweichen von dem Standard nicht möglich ist, handelt es sich um erzwungenen Schutz.

Im Folgenden sollen einige Beispiele herausgegriffen werden, mit denen der Staat seiner Pflicht zur Verhinderung nicht selbstbestimmter Preisgabe nachkommt. Angesichts des weiteren Einschätzungs- und Beurteilungsspielraums, den der Staat bei der Erfüllung seiner Schutzpflichten hat, besteht regelmäßig keine verfassungsrechtliche Pflicht, exakt die im Folgenden dargestellten Maßnahmen zu treffen. Sie stellen jeweils lediglich eine Möglichkeit dar, die der Staat ergreifen darf.

Der Schutz bei fehlender Einsichtsfähigkeit erfolgt, indem beispielsweise Jugendliche Einwilligungen nicht erteilen können, selbst wenn sie wollen. Die datenschutzrechtliche Einwilligung wird überwiegend als Realakt gewertet, ihre Wirksamkeit mithin an die Einsichtsfähigkeit der Handelnden geknüpft.[119] Die Gegen-

---

[116] *Kutscha*, Grundrechtlicher Persönlichkeitsschutz bei der Nutzung des Internets, DuD 2011, 461, 464.

[117] St. Rspr., seit: BVerfGE 88, 203 (254 ff.); siehe oben Kapitel 5,A.IV.

[118] Europäische Strategie für ein besseres Internet für Kinder vom 2.5.2012, 13; dazu: *Europäischer Datenschutzbeauftragter*, Stellungnahme 17.7.2012, 7. Der nicht verabschiedete § 13a Abs. 1 Satz 5 TMG-E sah vor, dass Nutzern, die bei der Erhebung ihrer personenbezogenen Daten ein Alter von unter 16 Jahren angegeben haben, eine Änderung der Voreinstellungen erst ermöglicht wird, wenn sie das Alter von 16 Jahren erreichen, Entwurf eines Gesetzes zur Änderung des Telemediengesetzes, BT-Drs. 17/6765 v. 3.8.2011.

[119] *Spindler/Nink*, in: Spindler/Schuster (Hrsg.), Recht der elektronischen Medien, 2015, § 4a BDSG, Rn. 3 f. m. w. N. und *Zscherpe*, Anforderungen an die datenschutzrechtliche Einwilligung im Internet, MMR 2004, 723, 724.

meinung geht zwar von der rechtsgeschäftlichen Natur der Einwilligung aus, stellt jedoch auf die Einsichtsfähigkeit anstelle der Geschäftsfähigkeit ab, da sonst die Minderjährigen durch die fehlende Preisgabemöglichkeit in ihrer Persönlichkeitsentfaltung eingeschränkt würden.[120] Wenn beide Ansichten im Ergebnis ohnehin das Kriterium der Einsichtsfähigkeit verwenden, erscheint es konsequenter, die Einwilligung von Beginn an als Realakt einzuordnen.

Überzeugend ist es, die Einsichtsfähigkeit im Rahmen der hier interessierenden elektronischen Datenverarbeitung bis zum siebten Lebensjahr abzulehnen nach dem Gedanken des § 828 Abs. 1 BGB sowie bis zum 14. Lebensjahr zu verneinen in Anlehnung an § 19 StGB. Auch für das Alter zwischen 14 und 16 wird die Einsichtsfähigkeit aufgrund der Komplexität der Sachverhalte und der mangelnden Lebenserfahrung der Preisgebenden im Zweifel noch nicht vorliegen.[121] So hat jüngst das Oberlandesgericht Hamm die Einwilligungsfähigkeit Fünfzehnjähriger in Datenspeicherung und Datenerhebung zur Werbezwecken grundsätzlich abgelehnt.[122] Zu weitreichend ist jedoch die Forderung des 69. Deutschen Juristentags, auch bei einsichtsfähigen Minderjährigen immer die Zustimmung der gesetzlichen Vertreter und die Einwilligung der einsichtsfähigen Minderjährigen zu verlangen.[123] Art. 8 Abs. 1 EU-DS-GVO-E hingegen setzt, in Übereinstimmung mit Sec. 1302 f. des in den Vereinigten Staaten maßgeblichen Children's Online Privacy Protection Act,[124] die Schwelle bei 13 Jahren an. Kindern und Jugendlichen vor Erreichen dieser Altersgrenze ist die eigenständige informationelle Preisgabe versagt. Angesichts der Schwierigkeit der im Internetkontext zu treffenden Entscheidungen erscheint es allerdings ratsam, die Einsichtsfähigkeit auch nach Erreichen des 13. Lebensjahres jedenfalls bis zum 16. Lebensjahr abzulehnen.

Zur Erfüllung der Schutzpflicht im Falle fehlender Wahlmöglichkeit gibt es ebenfalls zahlreiche Beispiele:

Das Verbraucherschutzrecht und insbesondere § 309 BGB verbieten eine Reihe von Klauseln in Allgemeinen Geschäftsbedingungen, die zuungunsten der Verbraucher von den gesetzlichen Vorschriften abweichen würden.

Prägnant ist § 28a Abs. 2 Satz 4 BDSG, nach dem die Übermittlung von Daten über Verhaltensweisen der Betroffenen, die im Rahmen eines vorvertraglichen Vertrauensverhältnisses mit einem Kreditinstitut der Herstellung von Markttranspa-

---

[120] *Rogosch*, Die Einwilligung im Datenschutzrecht, 2013, 49 und *Simitis*, in: ders. (Hrsg.), Bundesdatenschutzgesetz, 2014, § 4a, Rn. 20.

[121] So auch: *Spindler/Nink*, in: Spindler/Schuster (Hrsg.), Recht der elektronischen Medien, 2015, § 4a, Rn. 3 f. m. w. N.; zum Schutz Minderjähriger in sozialen Netzwerken: *Jandt/Roßnagel*, Social Networks für Kinder und Jugendliche, MMR 2011, 637, 638 ff.

[122] OLG Hamm ZD 2013, 29.

[123] *Deutscher Juristentag*, Beschlüsse des 69. Deutschen Juristentags, 2012, 25 auf Basis von: *Spindler*, Persönlichkeitsschutz im Internet, in: Ständige Deputation des Deutschen Juristentages (Hrsg.), Verhandlungen des 69. Deutschen Juristentages, 2012, I, S. F1–F136 ff.

[124] 15 U.S.C. § 6501 ff., umgesetzt durch die Children Online Privacy Protection Rule, 16 C.F.R. § 312.

renz dienen, an Auskunfteien auch mit Einwilligung der Betroffenen unzulässig ist. Dadurch wird unabhängig vom Willen der Betroffenen verhindert, dass die erste Kontaktaufnahme der Kunden zu dem Kreditinstitut negative Auswirkungen auf ihren Scorewert bei Auskunfteien wie der Schutzgemeinschaft für allgemeine Kreditsicherung (SCHUFA) hat.[125] Die Verfassungsmäßigkeit von § 28a Abs. 2 Satz 4 BDSG ist zwar nicht unumstritten.[126] Angesichts der Bedeutung, die die Scorewerte der Auskunfteien für das Alltagsleben der Betroffenen haben und angesichts der ausgesprochen schwachen Verhandlungsposition, in der sich Kreditsuchende häufig befinden, ist jedoch entgegen der Kritik in der Literatur von einer fehlenden Wahlmöglichkeit auszugehen und die Verfassungsmäßigkeit des § 28a Abs. 2 Satz 4 BDSG gerade als Ausdruck der hier diskutierten verfassungsrechtlichen Schutzpflicht zu bejahen.

Nach § 28 Abs. 3b BDSG verboten ist die Kopplung eines Vertragsschlusses an die Einwilligung in die Verarbeitung oder Nutzung personenbezogener Daten für Adresshandel oder Werbung, wenn den Betroffenen ein anderer Zugang zu gleichwertigen vertraglichen Leistungen ohne die Einwilligung nicht oder nicht in zumutbarer Weise möglich ist. Ein Verstoß dagegen stellt eine Ordnungswidrigkeit nach § 43 Abs. 2 Nr. 5a BDSG dar. Ähnliches gilt auch im Anwendungsbereich des Telekommunikationsgesetzes (§ 95 Abs. 5 Satz 2 TKG) und des Telemediengesetzes (§ 12 Abs. 3 TMG in Verbindung mit § 28 Abs. 3b Satz 2 BDSG).

Weitere Informationserhebungsverbote statuieren § 18 Abs. 1 Satz 1 Nr. 2 Gendiagnostikgesetz (Versicherer dürfen von den Versicherten keine Ergebnisse oder Daten aus genetischen Untersuchungen oder Analysen entgegennehmen) und § 19 Nr. 2 Gendiagnostikgesetz (Arbeitgeber dürfen von den Bewerbern und Arbeitnehmern keine Ergebnisse genetischer Untersuchungen oder Analysen entgegennehmen). Auch dieser aufgezwungene Schutz ist jedoch nicht unumstritten.[127] Zwar lässt sich nicht pauschal davon ausgehen, dass Versicherte, Bewerber oder Arbeitnehmer bei Verhandlungen über die Preisgabe ihrer Gendaten immer unterliegen, doch besteht jedenfalls eine signifikante entsprechende Gefahr. Angesichts der gravierenden und dauerhaften Risiken, die die Preisgabe von Gendaten mit sich bringen kann, muss bereits der begründete Verdacht der fehlenden Wahlmöglichkeit ausreichen, um solche Preisgaben zu verhindern. Es kann zudem nicht im Sinne der Gesellschaft liegen, dass eine Vielzahl an Versicherten, Bewerbern und Arbeitnehmern gegen ihren Willen ihre Gendaten preisgibt. Die gegenteilige Kritik verdient daher keine Zustimmung.

Das begrenzte Fragerecht der Arbeitgeber nach einer etwaigen Schwangerschaft der Bewerberinnen oder Arbeitnehmerinnen stellt eine Mischform dar, indem es in

---

[125] Gola/Schomerus-BDSG/*Gola/Schomerus*, 2015, § 28a BDSG, Rn. 16.

[126] Ablehnend: *Rogosch*, Die Einwilligung im Datenschutzrecht, 2013, 101.

[127] *Nettesheim* hält diese Verbot jedenfalls für verfassungsrechtlich nicht geboten: *Nettesheim*, Grundrechtsschutz der Privatheit, in: Höfling (Hrsg.), Der Schutzauftrag des Rechts, 2011, 7, 42.

bestimmten Fällen die Informationserhebung durch die Arbeitgeber verhindert, ohne jedoch die freiwillige Mitteilung durch die Befragten auszuschließen.[128]

Hinzu kommen gesetzliche Vorschriften, die zwar nicht die Preisgabe verhindern, den Nutzern jedoch zukünftige Optionen, auf die Preisgabe zu reagieren, offenhalten. Beispielsweise ist ein Verzicht auf die Möglichkeit zum Widerruf der datenschutzrechtlichen Einwilligung nicht zulässig.[129] Nach § 6 Abs. 1 BDSG können die Auskunftsrechte aus §§ 19, 34 BDSG sowie die Rechte auf Berichtigung, Löschung oder Sperrung nach §§ 20, 35 BDSG nicht durch Rechtsgeschäft ausgeschlossen oder beschränkt werden. Den Betroffenen steht die Preisgabe ihrer Daten frei, jedoch mit der Maßgabe, dass ihnen auch danach noch bestimmte Formen der Kontrolle über ihre Daten verbleiben müssen.

Den genannten Normen ist gemein, dass sie den Preisgebenden Privatheit aufzwingen, um sie vor nicht selbstbestimmter Preisgabe zu schützen. Dabei dienen sie der Erfüllung der entsprechenden staatlichen Schutzpflicht.

VII. Pflicht zum Schutz von Allgemeinwohlbelangen

Weiter könnte eine Pflicht zum Schutz von Allgemeinwohlbelangen bestehen. Voraussetzungen sind wiederum die Beeinträchtigung von Grundrechten durch Private sowie die Schutzbedürftigkeit der Rechtsträger.

Informationelle Preisgabe kann zunächst insbesondere Gefahren für die informationelle Privatheit Dritter erzeugen, wenn aus preisgegebenen personenbezogenen Daten auch Rückschlüsse auf Dritte möglich sind.[130] Dadurch werden Belange beeinträchtigt, die durch das Recht auf informationelle Selbstbestimmung der Dritten geschützt sind.

Zwar sind die Preisgebenden nicht selbst an Grundrechte gebunden, doch könnte der Staat das Recht auf informationelle Selbstbestimmung der Dritten bei der Frage nach einer Pflicht zur Verhinderung informationeller Preisgabe berücksichtigen müssen. Der Schutz vor Übergriffen Dritter ist die typische Schutzpflichtenkonstellation, die sich schon zurückführen lässt auf die Philosophie *Mills*, der staatliches Einschreiten immer dann zulässt, wenn das in Rede stehende Verhalten den Interes-

---

[128] *Link*, in: Schaub (Hrsg.), Arbeitsrechtshandbuch, 2013, § 26, Rn. 16 ff. m. w. N. Ungenau ist es daher, das begrenzte Fragerecht undifferenziert als Beispiel eines unveräußerlichen Rechts einzuordnen, so aber: *Fisahn*, Ein unveräußerliches Grundrecht am eigenen genetischen Code, ZRP 2001, 49, 54.

[129] *Bräutigam*, Das Nutzungsverhältnis bei sozialen Netzwerken, MMR 2012, 635, 636; *Helfrich*, in: Hoeren/Sieber/Holznagel (Hrsg.), Handbuch Multimedia-Recht, 2015, 16.1, Rn. 77; *Rogosch*, Die Einwilligung im Datenschutzrecht, 2013, 133 und *Traut*, in: Thüsing (Hrsg.), Beschäftigtendatenschutz und Compliance, 2014, § 5, Rn. 33. Die Widerruflichkeit der Einwilligung ergibt sich aus dem Recht auf informationelle Selbstbestimmung und ist kodifiziert in § 13 Abs. 2 Nr. 4 TMG.

[130] Siehe oben Kapitel 3,A.III.1; zur Zuordnung der Rechte Dritter zu den Allgemeinwohlbelangen siehe oben Kapitel 3,A.III.

senkreis Anderer schneidet.[131] Die Freiheitsausübung der Einzelnen findet ihre Grenzen in der Beeinträchtigung der Freiheiten Anderer und kann niemals die Befugnis umfassen, in die geschützten Rechtssphären von Anderen ohne rechtfertigenden Grund einzugreifen.[132] Die Protektion Dritter vor Übergriffen verlangt schließlich auch die Ökonomische Analyse des Rechts. Solche Beeinträchtigungen lassen sich als Externalitäten klassifizieren: Die Kosten eines Geschäfts treffen nicht die Beteiligten, sondern Unbeteiligte. Um ein Marktversagen zu verhindern, muss der Staat korrigierend eingreifen.[133] Daraus folgt der Auftrag an den Staat, in einem mehrpoligen Grundrechtsverhältnis die widerstreitenden Interessen in praktische Konkordanz zu bringen. Ausschlaggebend für das Entstehen von Schutzpflichten ist erneut die Schutzbedürftigkeit der Dritten. Soweit ein angemessenes Schutzniveau durch private Eigenvorsorge realisiert werden kann, besteht für weiter gehende staatliche Interventionen kein Anlass.[134] Die Prüfung der Schutzbedürftigkeit hat einzelfallbezogen stattzufinden. Für das Vorliegen der Schutzbedürftigkeit und das Entstehen der Schutzpflicht dürfte es aber jedenfalls sprechen, wenn die Dritten nichts von der Bedrohung wissen können oder sie rechtlich (etwa aufgrund eines Datentransfers aus dem Geltungsbereich des deutschen Datenschutzrechts heraus) oder faktisch keine Gegenmaßnahmen einleiten können.

Zur Erfüllung dieser Schutzpflicht gilt das Untermaßverbot[135] und dem Staat steht ein weiter Gestaltungsspielraum zu. Da ein mehrpoliges Grundrechtsverhältnis vorliegt, muss eine Abwägung zwischen den kollidierenden Grundrechtspositionen durchgeführt werden, regelmäßig also zwischen dem Recht auf informationelle Selbstbestimmung der Preisgebenden[136] und dem Recht auf informationelle Selbstbestimmung der Dritten.

Im Rahmen der Abwägung ist insbesondere zu beachten, wie stark die jeweiligen Grundrechte beeinträchtigt werden. Maßnahmen zur Unterstützung informationellen Selbstschutzes belasten die Grundrechte der Preisgebenden nicht, sind jedoch unter Umstände nicht wirksam genug. Maßnahmen der Entscheidungsarchitektur sind für die Preisgebenden weniger einschneidend als der Schutz durch Zwang, aber regelmäßig auch weniger wirksam. Nach Abwägung im Einzelfall ist das mildeste wirksame Mittel zu wählen, das die Grundrechte der Preisgebenden nicht unangemessen beeinträchtigt. In der Regel wird erzwungener Schutz das einzige wirksame Mittel sein.

---

[131] *Mill*, Über die Freiheit, 2010 (Original: 1859), 20.

[132] BVerfGE 39, 1 (43).

[133] *Cooter/Ulen*, Law & Economics, [6]2010, 39 f.; siehe unten Kapitel 7,A.II.

[134] *Trute*, Verfassungsrechtliche Grundlagen, in: Roßnagel (Hrsg.), Handbuch Datenschutzrecht, 2003, 156, 181, Rn. 51.

[135] St. Rspr., seit: BVerfGE 88, 203 (254 ff.); siehe oben Kapitel 5,A.IV.

[136] Der Fokus der Arbeit liegt auf der Konstellation, in der die Preisgebenden sie betreffende Daten preisgeben, die auch Rückschlüsse auf Andere zulassen. Hier ist primär das Recht auf informationelle Selbstbestimmung der Preisgebenden tangiert. Denkbar sind aber je nach Sachverhalt auch hier nicht behandelte Überschneidungen mit der Meinungs- oder Berufsfreiheit.

Jedenfalls muss der Staat eine Rechts- und Verfahrensordnung bereitstellen, die es den betroffenen Dritten ermöglicht, nachträglich gegen sie beeinträchtigende Preisgabe vorzugehen sowie im Rahmen des Möglichen entsprechende Preisgabe ex ante zu verhindern. Zu denken ist hier beispielsweise an die Unterlassungsansprüche aus § 1004 Abs. 1 BGB analog.

Hinzu treten Regelungen, die bestimmte Preisgabe von vornherein verbieten, wie das Verbotsprinzip, aber etwa auch Verschwiegenheits- oder Geheimhaltungspflichten von Ärzten, Anwälten et cetera. Verstöße von Berufs- und Amtsgeheimnisträgern gegen diese Pflichten werden strafrechtlich durch § 203 StGB sanktioniert.

Weiter können durch informationelle Preisgabe die verfassungsrechtlich abgesicherten Interessen an gesellschaftlichem Fortschritt und der Funktionsfähigkeit der Demokratie gefährdet werden. Diese Interessen erfahren jedoch überwiegend keinen Schutz durch konkrete Grundrechte, sondern sind vielmehr als übergeordnete Werte oder Staatsstrukturprinzipien abgesichert. Abstrakte Allgemeinwohlbelange können daher zwar unter Umständen als Rechtfertigungsgründe für Grundrechtseingriffe dienen,[137] Schutzpflichten können jedoch mangels beeinträchtigter konkreter Grundrechtsträger aus ihnen nicht erwachsen.

VIII. Umsetzung der Schutzpflicht im inter- und transnationalen Kontext

Informationelle Preisgabe im Internet findet häufig über internationale Anbieter statt, sodass der internationalen Umsetzung der Schutzpflicht große Bedeutung zukommt.

Der Schutz der Grundrechte deutscher Bürger im Internet wird erschwert dadurch, dass die zugrunde liegenden Sachverhalte typischerweise Auslandsbezug aufweisen.[138] Die Grundrechtsübergriffe finden häufig nicht (nur) auf dem Staatsgebiet Deutschlands statt. Hinzu kommt, dass Bedrohungen regelmäßig nicht von deutschen, sondern von ausländischen verantwortlichen Stellen ausgehen.

Es stellt sich daher die Frage nach der Umsetzung der Schutzpflichten in diesen Konstellationen. Als Ausnahme vom völkerrechtlichen Territorialprinzip beanspruchen die Grundrechte jedenfalls dann Geltung, wenn ein Inländerbezug besteht.[139] Jedenfalls gegeben ist dieser, wenn die Betroffenen auf deutschem Staatsgebiet Bedrohungen durch ausländische verantwortliche Stellen ausgesetzt sind.[140] Den Anwendungsbereich deutschen Datenschutzrechts definiert § 1 Abs. 2, 5 BDSG.[141]

---

[137] Siehe unten Kapitel 6,A.III.

[138] Zur zugrunde liegenden Problematik: *Thomé*, Zweiter Teil, in: Kutscha/Thomé (Hrsg.), Grundrechtsschutz im Internet?, 2013, 101, 118 ff.

[139] *Schliesky/Hoffmann/Luch u. a.*, Schutzpflichten und Drittwirkung im Internet, 2014, 67.

[140] Das Recht auf informationelle Selbstbestimmung ist nach dem Wortlaut von Art. 2 Abs. 1 und Art. 1 Abs. 1 GG ein Jedermanns-Grundrecht, sodass es nicht nur für deutsche Staatsangehörige gilt.

[141] Dazu: *Berger/Kraska*, Datenschutz im Web 2.0, 2012; *Beyvers/Herbrich*, Das Niederlas-

Soweit die Grundrechte deutscher Staatsbürger jedoch durch Verhalten bedroht werden, welches sich dem Herrschaftsbereich deutscher Gesetzgebung entzieht, stellen sich die Fragen nach Existenz und Umfang der Schutzpflicht.

Im Falle von völkerrechtswidrigem Verhalten einer fremden Hoheitsgewalt auf fremdem Hoheitsgebiet gegenüber deutschen Staatsbürgern steht der Bundesrepublik völkerrechtlich das Recht zu, ihren Staatsbürgern diplomatischen Schutz zu gewähren. Aus der Schutzpflicht hinsichtlich der bedrohten Rechtsgüter kann den betroffenen Bürgern zugleich ein Anspruch gegenüber der Bundesrepublik auf Ausübung des diplomatischen Schutzes erwachsen.[142] Überwachungsmaßnahmen ausländischer Geheimdienste, deren Rechtmäßigkeit umstritten ist und die sich jedenfalls nicht innerhalb des von den Preisgebenden intendierten Verwendungszwecks der Daten befinden, bleiben in der vorliegenden Arbeit – die sich ausschließlich den rechtmäßigen Folgen der Preisgabe widmet – außer Betracht. Die Konstellation des aus der Schutzpflicht erwachsenden Anspruchs auf Ausübung diplomatischen Schutzes kann damit hier vernachlässigt werden.

Darüber hinaus trifft den Staat jedoch eine modifizierte Schutzpflicht, um auch bei Auslandssachverhalten den bestmöglichen Schutz seiner Bürger zu erreichen.

Er hat zunächst den Auftrag, auf Ebene der Europäischen Union auf den Erlass und die Umsetzung von EU-Recht hinzuwirken, welches einen hohen Grundrechtsschutz erreicht. Derzeit gilt hier (noch) insbesondere die EU-Datenschutzrichtlinie. Wie der Europäische Gerichtshof jüngst entschied, ist sie auch anwendbar bei der Verarbeitung personenbezogener Daten durch außereuropäische Suchmaschinenbetreiber, wenn diese Verarbeitung im Rahmen der Tätigkeit einer europäischen Niederlassung stattfindet. Dies ist selbst dann der Fall, wenn die europäische Niederlassung in die tatsächliche Datenverarbeitung überhaupt nicht einbezogen ist, aber durch wirtschaftliche Aktivitäten wie das Anbieten von Werbeflächen in einer Weise tätig wird, die einen direkten Bezug zur Europäischen Union hat (Marktortprinzip).[143] Eine Regelung in diesem Sinne enthält auch Art. 3 Abs. 2 EU-DS-GVO-E.

Im inter- und transnationalen Kontext gebietet es die grundrechtliche Schutzpflicht, den Abschluss internationaler Verträge anzustreben, die den Grundrechtsschutz im Rahmen des Möglichen gewährleisten.[144] Soweit erforderlich, muss sich

---

sungsprinzip im Datenschutzrecht, ZD 2014, 558 ff. und *Hornung*, Europa und darüber hinaus, in: Hill/Schliesky (Hrsg.), Die Neubestimmung der Privatheit, 2014, 123, 130 f.

142 Zur verfassungsrechtlichen Einordnung dieser Schutzpflicht: *Isensee*, Das Grundrecht als Abwehrrecht und als staatliche Schutzpflicht, in: Isensee/Kirchhof (Hrsg.), Handbuch des Staatsrechts der Bundesrepublik Deutschland X, 2012, 413, 513 f., Rn. 212.

143 EuGH EuZW 2014, 541 (544).

144 *Greve*, Internetregulierung zwischen Grundrechtsermöglichung und Informationsrestriktion, DAJV Newsletter 2013, 164, 168; *Hoffmann-Riem*, Grundrechts- und Funktionsschutz für elektronisch vernetzte Kommunikation, 134 AöR (2009), 513, 538 ff.; *ders.*, Freiheitsschutz in den globalen Kommunikationsinfrastrukturen, JZ 2014, 53, 59 ff.; *Schaar*, Lässt sich die globale Internetüberwachung noch bändigen?, ZRP 2013, 214, 215 f. und *Schliesky/Hoffmann/Luch u. a.*, Schutzpflichten und Drittwirkung im Internet, 2014, 165 ff.

der deutsche Staat auch für den Beitritt der Europäischen Union zu entsprechenden internationalen Abkommen einsetzen. Der grundrechtliche Gewährleistungsauftrag gibt deutschen Hoheitsträgern dabei „rechtsnormative Orientierung für ihr Verhalten in den trans- und internationalen Handlungsarenen.“[145] Die Bemühungen im Klimaschutzsektor können zum Beispiel genommen werden, auch im Bereich des Datenschutzes durch Abschluss völkerrechtlicher Verträge Schutz zu garantieren.[146] Wie effektiv ein solcher Schutz ist, hängt jedoch davon ab, mit welchen Sanktionsmechanismen auf Verstöße reagiert werden kann. Zieht ein Verstoß keine negativen Folgen nach sich, wird die Einhaltung des Abkommens fraglich sein, wodurch erhebliche Frustration insbesondere aufseiten der Bürger entstehen kann.

B. Schutzpflicht nach US-Verfassungsrecht

Anders als in Deutschland fungieren verfassungsmäßige Rechte in den Vereinigten Staaten nur als Abwehrrechte der Bürger gegen den Staat und haben keine Auswirkungen auf Privatrechtsverhältnisse.[147] Es gibt also, anders als in Deutschland, keine mittelbare Drittwirkung der Grundrechte. Die Zusatzartikel sind negativ formuliert und legen fest, was der Staat nicht darf, jedoch nicht, dass er etwas muss.[148]

Eine dogmatisch tief gehende Debatte um die Einführung von Schutzpflichten wird nicht geführt.[149] Sehr vereinzelt wird geäußert, auch das bestehende US-Recht ließe sich in einer Weise auslegen, die zu mehr Grundrechtswirkung zwischen Privaten führen würde als bisher. Dass trotzdem das Verhalten der Privaten regelmäßig keine verfassungsmäßigen Rechte der Betroffenen berühre, läge daran, dass Eingriffe gerade im Bereich der Redefreiheit in den USA viel schwieriger zu rechtfertigen seien als anderswo, sodass es regelmäßig an einer unzulässigen Beeinträchtigung der Rechte der Betroffenen fehle.[150] Sicherlich spielen auch die Voraussetzungen, unter denen ein Grundrechtseingriff in verschiedenen Rechtsordnungen gerechtfer-

---

145 *Hoffmann-Riem*, Freiheitsschutz in den globalen Kommunikationsinfrastrukturen, JZ 2014, 53, 60.

146 *Hoffmann/Schulz/Borchers*, Grundrechtliche Wirkungsdimensionen im digitalen Raum, MMR 2014, 89, 93.

147 *Lange*, Grundrechtsbindung des Gesetzgebers, 2010, 416 ff. m. w. N. und *Loewenstein*, Verfassungsrecht und Verfassungspraxis der Vereinigten Staaten, 1959, 479 f.

148 *Abernathy*, Law in the United States, 2006, 449.

149 Zu diesem Ergebnis kommen auch: *Giegerich*, Privatwirkung der Grundrechte in den USA, 1992, 451 ff.; *Lange*, Grundrechtsbindung des Gesetzgebers, 2010, 416 ff.; vgl.: *Wittmann*, Der Schutz der Privatsphäre vor staatlichen Überwachungsmaßnahmen durch die US-amerikanische Bundesverfassung, 2014, 38 f.

150 *Gardbaum* kommt in seiner Untersuchung der mittelbaren Drittwirkung der Grundrechte in den USA, Deutschland und Kanada zu dem Schluss: „[I]f and to the extent that constitutional rights do have less impact on private actors in the United States than in other countries rejecting direct horizontality, it is neither due to an exceptional, more vertical structural position on the scope of rights nor to how the state action doctrine operates. It is exclusively because of substantive differences in the rights themselves and their interpretation; that is, not because fewer laws are

tigt werden kann, eine Rolle bei der Beantwortung der Frage, ob der Staat privates Verhalten zum Schutz betroffener Grundrechtsträger verhindern muss. Doch fundamentaler führt bereits die gänzliche Ablehnung von Schutzpflichten dazu, dass der Staat nicht in die Verhältnisse Privater untereinander einzugreifen hat.

Die Frage nach der Existenz von Schutzpflichten taucht an einzelnen Stellen in Rechtsprechung und Literatur auf, wird jedoch sofort ablehnend beantwortet.

In der Entscheidung Shelley v. Kraemer aus dem Jahr 1948 führt der U.S. Supreme Court aus, dass ein Schutz gegen private Handlungen nicht besteht, egal, wie diskriminierend oder unrechtmäßig sie sind.[151] Im zugrunde liegenden Fall war den Klägern aufgrund ihrer schwarzen Hautfarbe durch einen zivilrechtlichen Vertrag der Eigentümergemeinschaft verboten wurde, das von ihnen erworbene Grundstück zu beziehen.

Eine behauptete Pflicht, armen Bürgern eine angemessene Unterkunft zu gewährleisten, wurde ebenso verneint mit der Begründung: „[T]he Constitution does not provide judicial remedies for every social and economic ill. We are unable to perceive in that document any constitutional guarantee of access to dwellings of a particular quality".[152]

In der Entscheidung DeShaney v. Winnebago County Dept. of Social Services war der U.S. Supreme Court mit der Klage eines Kindes befasst, das von seinem Vater wiederholt massiv misshandelt wurde, obwohl die Mutter mehrfach vergeblich versucht hatte, ein staatliches Einschreiten dagegen zu erwirken. Das Kind macht eine Verletzung des substanziellen Rechtsstaatlichkeitsgebots geltend, da der Staat sein Recht auf körperliche Integrität verletzt habe, indem er ihm keinen Schutz bot („failing to intervene to protect him against his father's violence").[153] Übertragen auf die deutsche Grundrechtsdogmatik wird also eine Verletzung der Schutzpflicht hinsichtlich der körperlichen Integrität behauptet. Eine solche lehnt der U.S. Supreme Court jedoch in klaren Worten ab: „But nothing in the language of the Due Process Clause itself requires the State to protect the life, liberty, and property of its citizens against invasion by private actors. The Clause is phrased as a limitation on the State's power to act, not as a guarantee of certain minimal levels of safety and security. It forbids the State itself to deprive individuals of life, liberty, or property without 'due process of law,' but its language cannot fairly be extended to impose an affirmative obligation on the State to ensure that those interests do not come to harm through other means."[154] Der Zweck der Due-Process-Klauseln sei es „to protect the people from the State, not to ensure that the State protected them from each other.

subject to constitutional rights scrutiny but because fewer laws may fail it.": *Gardbaum*, The Myth and the Reality of American Constitutional Exceptionalism, 107 Mich. L. Rev. (2009), 391, 442 f.

151 Eine Analyse der vorangegangenen und nachfolgenden Entscheidungen liefert: *Giegerich*, Privatwirkung der Grundrechte in den USA, 1992, 284 ff.

152 Lindsey v. Normet, 405 U.S. 56, 74 (1972).

153 DeShaney v. Winnebago County Dept. of Social Services, 489 U.S. 189, 189 (1989).

154 DeShaney v. Winnebago County Dept. of Social Services, 489 U.S. 189, 195 (1989).

The Framers were content to leave the extent of governmental obligation in the latter area to the democratic political processes.“[155]

In dem Sachverhalt, der der Entscheidung Town of Castle Rock, Colo. v. Gonzales zugrunde lag, hatte der Staat eine einstweilige Verfügung, die dem Vater den Umgang mit seinen Kindern untersagte, nicht durchgesetzt und war auch nicht eingeschritten, als der Vater die Kinder entführte und später ermordete. Die Mutter behauptete auf Basis des durch die Due-Process-Klauseln statuierten Verbots, Bürgern ihr Eigentum ohne Einhaltung des Rechtsstaatlichkeitsgebots zu nehmen, ein Recht auf Durchsetzung der einstweiligen Verfügung. Nach Ansicht des U.S. Supreme Courts besteht jedoch kein Eigentumsinteresse an der Durchsetzung einstweiliger Verfügungen.[156] Mit keinem Wort angesprochen wird jedoch die – aus deutscher Sicht auf der Hand liegende – Frage, ob aus dem Recht der Kinder auf Leben eine Pflicht zum staatlichen Einschreiten erwuchs.

Der Staat soll sich weitestmöglich aus den Angelegenheiten der Bürger heraushalten. Daher wurde beispielsweise auch eine staatliche Pflicht, Unfallopfern zu helfen, mit der Begründung abgelehnt: „The men who wrote the Bill of Rights were not concerned that government might do too little for the people but that it might do too much to them.“[157] Im zugrunde liegenden Sachverhalt waren die Unfallopfer gestorben, während der anwesende Polizeibeamte den Verkehr um die Unfallstelle herumleitete.

Die ablehnende Haltung der US-Gerichte gegenüber dem Konzept der Schutzpflichten zeigt sich auch im Bereich der Schwangerschaftsabbrüche. Das Right to Privacy garantiert Frauen das Recht zur Abtreibung.[158] Dieses gilt jedoch nicht absolut, sondern kann zur Erreichung eines zwingenden staatlichen Zweckes eingeschränkt werden. Ein solcher Zweck kann der Schutz ungeborenen Lebens sein.[159] Anders als im deutschen Recht[160] wird dabei jedoch keine Schutzpflicht zugunsten des ungeborenen Lebens erwogen, sondern sein Schutz lediglich zur Eingriffsrechtfertigung herangezogen. Das Right to Privacy limitiert staatliche Maßnahmen, die die Frauen bei der Durchführung eines Schwangerschaftsabbruchs behindern würden, wie strafbewehrte Abtreibungsverbote[161] oder das Auferlegen eines unverhältnismäßigen Hindernisses („undue burden“) bei der Entscheidung zum Schwangerschaftsabbruch durch Mitteilungspflichten gegenüber dem Ehemann.[162] Ob es ge-

[155] DeShaney v. Winnebago County Dept. of Social Services, 489 U.S. 189, 196 (1989).

[156] Town of Castle Rock, Colo. v. Gonzales, 545 U.S. 748, 768 (2005).

[157] Jackson v. City of Joliet, 715 F.2d 1200, 1203 (7th Cir. 1983).

[158] Roe v. Wade, 410 U.S. 113 (1973) und Planned Parenthood of Southeastern Pennsylvania v. Casey, 505 U.S. 833 (1992); siehe oben Kapitel 3,C.I.3.a).

[159] Roe v. Wade, 410 U.S. 113, 154 (1973).

[160] Erstmalige verfassungsgerichtliche Anerkennung in Deutschland fand das Konzept der grundrechtlichen Schutzpflicht just am Beispiel des Schutzes des ungeborenen Lebens vor Abtreibung: BVerfGE 39, 1 (42) und 88, 203 (252); siehe oben Kapitel 5,A.II.

[161] Roe v. Wade, 410 U.S. 113 (1973).

[162] Planned Parenthood of Southeastern Pennsylvania v. Casey, 505 U.S. 833 (1992).

gen das Right to Privacy verstößt, wenn der Staat durch überzogene Anforderungen an Abtreibungsärzte und -kliniken de facto die Schließung eines Großteils der Kliniken in einem Bundesstaat herbeiführt, bleibt entgegen der erstinstanzlichen Ansicht[163] offen, da der Fünfte Circuit Court jedenfalls den Nachweis nicht erbracht sah, dass die Erschwerung von Abtreibungen den einzigen Gesetzeszweck darstellten.[164] Gegenstände dieser Verfahren sind jedoch Regelungen, die den Frauen die Nutzung privater Abtreibungskliniken erschweren würden.

Eine staatliche Pflicht, den Schwangeren Möglichkeiten zum Schwangerschaftsabbruch zur Verfügung zu stellen und ihnen so die Ausübung ihres Rechts auf Abtreibung zu ermöglichen, lehnt der U.S. Supreme Court hingegen in ständiger Rechtsprechung ab:[165]

So begegnet das Unterlassen der Finanzierung von Abtreibungen bei gleichzeitiger Finanzierung von Geburten keinen Bedenken: „There is a basic difference between direct state interference with a protected activity and state encouragement of an alternative activity consonant with legislative policy. Constitutional concerns are greatest when the State attempts to impose its will by force of law; the State's power to encourage actions deemed to be in the public interest is necessarily far broader."[166]

In einer anschließenden Entscheidung wird eine Schutzpflicht abgelehnt hinsichtlich der Frage, ob der Staat verpflichtet ist, indigenen Frauen finanzielle Unterstützung zur Durchführung medizinisch notwendiger Schwangerschaftsabbrüche zu gewähren: „[I]t simply does not follow that a woman's freedom of choice carries with it a constitutional entitlement to the financial resources to avail herself of the full range of protected choices. [… A]lthough government may not place obstacles in the path of a woman's exercise of her freedom of choice, it need not remove those not of its own creation. […] Although Congress has opted to subsidize medically necessary services generally, but not certain medically necessary abortions, [… an] indigent woman [is left] with at least the same range of choice in deciding whether to obtain a medically necessary abortion as she would have had if Congress had chosen to subsidize no health care costs at all."[167]

Dabei kann der Staat selbst bei grundlegenden Dienstleistungen wie staatlichen Krankenhäusern rechtlich zulässiges, aber moralisch abgelehntes Verhalten unterlassen: „Missouri's decision to use public facilities and employees to encourage

---

163 Whole Woman's Health v. Lakey, Memorandum Opinion, 46 F.Supp.3d 673, 683 f. (W.D. Tex. 2014).

164 Whole Woman's Health v. Cole, WL 3604750, S. 34 (5th Cir. 2015); wohl im Widerspruch zu: Jackson Women's Health Organization v. Currier, 760 F.3d 448 (5th Cir. 2014).

165 Etwas zu optimistisch erscheint es daher, wenn aus der aktuellen Rechtsprechung im Bereich Schwangerschaftsabbruch der Schluss gezogen wird: „So ganz fremd scheint dem US-Verfassungsrecht hier eine grundrechtliche Schutzpflicht also vielleicht doch nicht zu sein.": *Unseld*, Mehr Schutzpflicht wagen?, 4.9.2014.

166 Maher v. Roe, 432 U.S. 464, 475 f. (1977).

167 Harris v. McRae, 448 U.S. 297, 316 (1980).

childbirth over abortion places no governmental obstacle in the path of a woman who chooses to terminate her pregnancy, but leaves her with the same choices as if the State had decided not to operate any hospitals at all.“[168]

Zwar verbietet es der durch den fünften und 14. Zusatzartikel gewährleistete Gleichbehandlungsgrundsatz, einigen Bürgern willkürlich den Schutz zu versagen, während andere Schutz erhalten. Diese, vom U.S. Supreme Court lediglich in einer Fußnote in DeShaney v. Winnebago County Dept. of Social Services getätigte, Feststellung[169] bleibt jedoch ohne signifikante Konsequenzen, wie die dargestellten Entscheidungen zur unterlassenen Unterstützung von Abtreibungen zeigen. Mit Zurückhaltung zu betrachten ist daher die Aussage, in den USA könnten sich Schutzpflichten aus dem Gleichbehandlungsgrundsatz ergeben, sodass die verfassungsrechtlichen Unterschiede zu Deutschland bei Weitem nicht so groß seien wie regelmäßig angenommen.[170] Zwar würde der Gleichbehandlungsgrundsatz tatsächlich eine Basis dafür bieten, Schutzpflichten jedenfalls dann anzuerkennen, wenn in vergleichbaren Situationen anderen Bedrohten Schutz zugestanden wurde. In ständiger Rechtsprechung entscheiden die Gerichte jedoch anders und fragen nur danach, ob die Beeinträchtigten schlechter stehen, als wenn der Staat niemandem geholfen hätte.[171]

Zusammenfassend stößt das Konzept der Schutzpflichten in den USA auf breite Ablehnung. Abgesehen von dem Schutz vor Sklaverei gemäß dem 13. Zusatzartikel[172] existieren keine verfassungsrechtlichen Schutzpflichten.

Die Bindung der Handelnden an die Zusatzartikel besteht nur bei Verhalten, das eine sogenannte State Action darstellt. Diese Terminologie geht zurück auf die richtungsweisenden Civil Rights Cases des U.S. Supreme Court: „It is State action of a particular character that is prohibited. Individual invasion of individual rights is not the subject matter“.[173] State Action liegt vor, wenn der Staat (entfernt vergleichbar

---

[168] Webster v. Reproductive Health Services, 492 U.S. 490, 491 (1989).

[169] DeShaney v. Winnebago County Dept. of Social Services, 489 U.S. 189, 197, Fn. 3 (1989).

[170] So aber: *Gardbaum*, The Myth and the Reality of American Constitutional Exceptionalism, 107 Mich. L. Rev. (2009), 391, 459.

[171] Harris v. McRae, 448 U.S. 297, 316 (1980) und Webster v. Reproductive Health Services, 492 U.S. 490, 491 (1989).

[172] Dieser lautet: „Neither slavery nor involuntary servitude, except as a punishment for crime whereof the party shall have been duly convicted, shall exist within the United States, or any place subject to their jurisdiction. Congress shall have power to enforce this article by appropriate legislation.“ Neben der Befugnis zur Bekämpfung existierender Sklaverei ergibt sich aus dem 13. Zusatzartikel auch eine Pflicht, dem Entstehen von Sklaverei vorzubeugen: Civil Rights Cases, 109 U.S. 3, 21 (1883). Das Verbot, sich in Sklaverei zu begeben, besitzt auch Geltung, wenn die Betroffenen voll geschäftsfähig sind, nicht bedroht oder getäuscht werden und sich weder irren noch Zwang ausgesetzt sind.

[173] Civil Rights Cases, 109 U.S. 3, 11, 13 (1883); zu Herleitung und aktuellem Stand: *Brugger*, Grundrechte und Verfassungsgerichtsbarkeit in den Vereinigten Staaten von Amerika, 1987, 30 ff.; *Buchner*, Informationelle Selbstbestimmung im Privatrecht, 2006, 7 ff.; *Giegerich*, Privatwirkung der Grundrechte in den USA, 1992, 191 ff.; zum Vergleich mit den deutschen Konzepten der Schutzpflicht und mittelbaren Drittwirkung: *Kumm/Ferreres Comella*, What Is So Special about

einem Beliehenen oder Verwaltungshelfer nach deutschem Verständnis) Private mit der Ausübung öffentlicher Tätigkeiten betraut[174] oder das private Verhalten eng mit dem staatlichen verbunden ist, insbesondere, indem der Staat unterstützend tätig wird.[175]

Im einfachen Recht spiegelt sich diese Dogmatik wieder in 42 U.S.C. § 1983, dem nach deutschem Verständnis entfernte Ähnlichkeit mit einem Amtshaftungsanspruch zukommt: „Every person who, under color of any statute, ordinance, regulation, custom, or usage […] subjects, or causes to be subjected, any citizen of the United States or other person within the jurisdiction thereof to the deprivation of any rights, privileges, or immunities secured by the Constitution and laws, shall be liable to the party injured in an action at law, suit in equity, or other proper proceeding for redress […]“. Anspruchsgegner („Every person“) können alle Angestellten auf Landes- oder kommunaler Ebene sein („any state or local official“) sowie Kommunalverwaltungen, wenn sie – über die Anstellung der unmittelbaren Schadensverursacher hinaus – am Eintritt des Schadens mitgewirkt haben.[176] Das Verhalten, das die verfassungsmäßigen Rechte beeinträchtigt, muss „under color of any statute, ordinance, regulation, custom, or usage“ erfolgen, verkürzt gesprochen also State Action darstellen.

Immer wieder wird versucht, Anbieter von Dienstleistungen, denen Relevanz für eine Vielzahl von Bürgern zukommt, als State Actors einzustufen und so ihre Grundrechtsbindung auszulösen. Auch diese Bemühungen fruchten jedoch nicht:

Der U.S. Supreme Court entschied in diese Richtung zwar zunächst, dass die Entscheidung einer Betreiberin von öffentlichem Nahverkehr, Radioprogramme zu spielen, State Action darstellt, wenn die Bahn unter öffentlicher Aufsicht betrieben wird.[177] Dies deutete daraufhin, dass die Anbieter öffentlicher Daseinsvorsorge als State Actors zu behandeln sein könnten.

In einer nachfolgenden Entscheidung wurde die Eigenschaft von Rundfunkveranstaltern – und damit von Anbietern öffentlich relevanter Dienstleistungen – als State Actors jedoch abgelehnt. Aus dem Umstand, dass bestimmte Handlungen staatlicherseits erlaubt oder nicht verboten worden sind, lässt sich noch keine Bindung der Privaten an die Redefreiheit schließen.[178]

Constitutional Rights in Private Litigation?, in: Sajó/Uitz (Hrsg.), The Constitution in Private Relations, 2005, 241, 266 ff.

[174] Marsh v. State of Alabama, 326 U.S. 501 (1946). Im zugrunde liegenden Fall hatte eine privat geführte Gemeinde („company-owned town“) das Verteilen von Flugblättern verboten. Dies stellte State Action dar.

[175] Burton v. Wilmington Parking Authority, 365 U.S. 715, 725 (1961). State Action liegt demnach vor, wenn ein Gaststättenbetreiber, der das einem Staatsgebäude zugehörige Restaurant gepachtet hat, Afroamerikaner diskriminiert.

[176] *Solove/Schwartz*, Information Privacy Law, [3]2009, 478.

[177] Public Utilities Commission of District of Columbia v. Pollak, 343 U.S. 451, 462 (1952).

[178] Columbia Broadcasting System, Inc. v. Democratic Nat. Committee, 412 U.S. 94, 119 (1973).

Ebenso stellt das Zurverfügungstellen von Energieversorgung keine State Action dar, da es sich dabei zwar um eine essenzielle öffentliche Dienstleistung („essential public service") handelt, die aber nicht notwendigerweise vom Staat angeboten werden muss.[179]

Angesichts der Bedeutung von Internetdienstanbietern und Suchmaschinen für den Lebensalltag vieler Bürger stellte sich die Frage, ob diese als State Actors zu behandeln sind und damit Grundrechtsbindung besteht. Dies wurde jedoch abgelehnt für Suchmaschinen, obwohl diese ihre Dienste der Öffentlichkeit anbieten.[180] Das Betreiben von Yahoo!-E-Mail-Gruppen stellt ebenfalls keine State Action dar, auch wenn das Internet in der Frühphase seiner Entwicklung öffentliche Zuschüsse erhalten hat, die auch Yahoo zugutekommen.[181] Gleiches gilt für die Tätigkeit von Internetdienstanbietern, auch wenn sie das Aufrufen von staatsfinanzierten Webseiten ermöglichen und ihre Dienste der Öffentlichkeit anbieten.[182]

Für Aufsehen gesorgt hat jüngst die in der Wissenschaft geäußerte Forderung nach einem „constitutional amendment to prohibit unreasonable searches and seizures of our persons and electronic effects, whether by the government or by private corporations like Google and AT&T." Zur Begründung wurde ausgeführt: „continuously tracking my location, whether by the government or AT&T, is an affront to my dignity. When every step I take on- and off-line is recorded, so an algorithm can predict if I am a potential terrorist or a potential customer, I am being objectified and stereotyped, rather than treated as an individual, worthy of equal concern and respect."[183] Staatliche und private Bedrohungen seien gleichzusetzen; vor beiden müsse die Verfassung anders als bisher ausdrücklich schützen. Bislang ist jedoch offen, ob dieser interessante Vorstoß, der immerhin vom Präsidenten des National Constitutional Center getätigt wurde, Konsequenzen haben wird.

Verpflichtender verfassungsrechtlicher Privatheitsschutz bleibt daher auf das Verhältnis Staat – Bürger beschränkt. Eine Ausnahme bietet lediglich die kalifornische Verfassung, deren Privatheitsschutz nach ständiger Rechtsprechung auch zwischen Privaten wirkt.[184] Dies sei im Informationszeitalter angesichts der faktischen Ge-

---

[179] Jackson v. Metropolitan Edison Co., 419 U.S. 345, 352 f. (1974).

[180] Langdon v. Google, Inc., 474 F.Supp.2d 622, 631 f. (D. Del. 2007).

[181] Murawski v. Pataki, 514 F.Supp.2d 577, 588 (S.D.N.Y. 2007).

[182] „We are unpersuaded by Green's contentions that AOL is transformed into a state actor because AOL provides a connection to the Internet on which government and taxpayer-funded websites are found, and because AOL opens its network to the public whenever an AOL member accesses the Internet and receives email or other messages from non-members of AOL": Green v. America Online (AOL), 318 F.3d 465, 472 (3d Cir. 2003); „Plaintiffs counter that AOL is a 'quasi-public utility' that 'involv[es] a public trust.' This claim is insufficient": Howard v. America Online Inc., 208 F.3d 741, 754 (9th Cir. 2000); Noah v. AOL Time Warner, Inc., 261 F.Supp.2d 532, 546 (E.D. Va. 2003) und Cyber Promotions, Inc. v. American Online, Inc., 948 F.Supp. 436, 443 f. (E.D. Pa. 1996).

[183] *Rosen*, Madison's Privacy Blind Spot, 18.1.2014.

[184] St. Rspr., statt vieler: Hill v. National Collegiate Athletic Assn., 865 P.2d 633, 644 (Cal. 1994).

fährdung durch Private notwendig, da das Right to Privacy sonst zur Farce würde, wie der kalifornische Appelate Court für den Ersten Distrikt ausführt: „Common experience with the ever-increasing use of computers in contemporary society confirms that the amendment was needed and intended to safeguard individual privacy from intrusion by both private and governmental action. That common experience makes it only too evident that personal privacy is threatened by the information-gathering capabilities and activities not just of government, but of private business as well. If the right of privacy is to exist as more than a memory or a dream, the power of both public and private institutions to collect and preserve data about individual citizens must be subject to constitutional control."[185] Da Kalifornien Sitz eines großen Teils der US-amerikanischen (IT-)Unternehmen ist, hat der kalifornische Privatheitsschutz dennoch spürbare Konsequenzen auf Nutzer auch im Rest der USA.

Eine Folge der fehlenden Pflicht zum Schutz der informationellen Privatheit der Bürger ist, dass in den Vereinigten Staaten, anders als in Deutschland, kein sektorenübergreifendes Datenschutzrecht existiert. Vielmehr bestehen einzelne sektorspezifische Regelungen, die sich zu einem Flickenteppich zusammensetzen. Dabei gibt es Regelungen zum Datenschutz im öffentlichen wie im privaten Bereich.[186] Beispielsweise enthält der Privacy Act of 1974 Datenschutzvorschriften für den öffentlichen Sektor,[187] der Fair Credit Reporting Act Vorschriften zum Umgang mit Finanzdaten im privaten Sektor.[188]

Eine verfassungsrechtliche Pflicht zur Verhinderung informationeller Preisgabe im Internet existiert in den Vereinigten Staaten nicht.

C. Vergleich

Hinsichtlich der Existenz einer Pflicht zur Verhinderung informationeller Preisgabe im Internet zeigen sich erhebliche Unterschiede zwischen Grundgesetz und US-amerikanischem Verfassungsrecht.

I. Evaluationsmaßstäbe

Es bestehen erhebliche Differenzen zwischen den beiden Rechtsordnungen hinsichtlich der Anerkennung verfassungsrechtlicher Schutzpflichten.

Die deutschen Grundrechte beinhalten eine objektiv-rechtliche Dimension: Ihre verfassungsrechtlichen Grundentscheidungen gelten für alle Bereiche des deutschen Rechts. Aus ihnen können sich Pflichten zum Schutz Einzelner vor privaten Übergriffen ergeben. Es obliegt dem Staat, die Privatrechtsordnung in grundrechts-

---

185 Wilkinson v. Times Mirror Corp., 215 Cal. App. 3d 1034, 1043 (Cal. App. 1 Dist. 1989).
186 Eine Übersicht bietet: *Genz*, Datenschutz in Europa und den USA, 2004, 50 ff.
187 5 U.S.C. § 552a.
188 15 U.S.C. § 1681 ff.

beachtender Weise zu gestalten. Er ist nicht (nur) „Grundrechtsfeind“, sondern (auch) „Grundrechtsfreund“.[189] Dies gilt auch für das Recht auf informationelle Selbstbestimmung und die Informationsfreiheit.

Voraussetzungen für das Entstehen einer Pflicht zur Verhinderung informationeller Preisgabe sind das Vorliegen von Beeinträchtigungen grundrechtlich geschützter Interessen durch privates Verhalten sowie die Schutzbedürftigkeit der betroffenen Grundrechtsträger. Zur Umsetzung der Schutzpflicht gilt das Untermaßverbot, der Staat darf also nicht untätig bleiben oder evident unzureichende Maßnahmen treffen. Hierbei hat er einen weiten Gestaltungsspielraum hinsichtlich der Form des Schutzes und des angestrebten Schutzniveaus.

Im Gegensatz zur deutschen Rechtslage kennt das US-Verfassungsrecht keine Schutzpflichten: Ihre Existenz wird in ständiger Rechtsprechung abgelehnt. Verfassungsmäßige Rechte wirken vielmehr ausschließlich im Staat-Bürger-Verhältnis. Zwar besteht eine Grundrechtsbindung, wenn Private als State Actor auftreten, doch wird diese Ausnahme restriktiv ausgelegt und auch verneint, wenn Private – wie beispielsweise Anbieter von Internetdiensten – Dienstleistungen erbringen, die von einer breiten Öffentlichkeit genutzt werden.

II. Analyse

Im deutschen Recht sind drei mögliche Schutzpflichtenkonstellationen zu unterscheiden:

Selbstbestimmt Preisgebenden fehlt es an der Schutzbedürftigkeit, selbst dann, wenn durch die Preisgabe der Menschenwürdekern des Rechts auf informationelle Selbstbestimmung berührt wird. Jedoch besteht eine Schutzpflicht zur Sicherung der Selbstbestimmung. Diese kann erfüllt werden durch Maßnahmen zur Unterstützung informationellen Selbstschutzes sowie nachrangig durch Entscheidungsarchitekturen.

Weiter muss erzwungener Schutz angewandt werden, um nicht selbstbestimmte Preisgabe zu verhindern.

Schließlich kann eine Schutzpflicht hinsichtlich der Rechte Dritter bestehen, wenn sich die Belange der durch die Preisgabe beeinträchtigten Dritten gegen die Grundrechte der Preisgebenden durchsetzen. Zwischen den widerstreitenden Grundrechten ist dann eine praktische Konkordanz herzustellen und ein geeignetes sowie erforderliches Mittel aus einer der drei Kategorien erzwungener Schutz, Unterstützung informationellen Selbstschutzes und Entscheidungsarchitekturen zu wählen. Regelmäßig wird erzwungener Schutz jedoch das einzig wirksame Mittel sein. Hinsichtlich abstrakter Allgemeinwohlbelange besteht keine Schutzpflicht.

Gerade im Internetkontext entziehen sich die zugrunde liegenden Sachverhalte häufig dem Geltungsbereich des Grundgesetzes. Es gilt dann eine modifizierte

[189] *Stern*, Die Schutzpflichtenfunktion der Grundrechte, DÖV 2010, 241, 244.

Schutzpflicht, nach der sich der Staat um die Schaffung eines schützenden Rechtsrahmens auf europäischer oder völkerrechtlicher Ebene bemühen muss.

Im liberalen Rechtssystem der Vereinigten Staaten hingegen stößt das grundgesetzliche Einwirken des Staates auf Privatrechtsverhältnisse auf Verwunderung. Dort bestehen auf bundesstaatlicher Ebene keinerlei Schutzpflichten, sodass auch keine Schutzpflicht hinsichtlich der durch informationelle Preisgabe im Internet entstehenden Gefahren existiert. Eine abweichende Rechtslage gilt nur für das Right to Privacy nach der kalifornischen Verfassung, das vergleichbar dem deutschen Ansatz auch zwischen Privaten wirkt.

Die fundamentalen Unterschiede zwischen den beiden Verfassungsordnungen lassen sich erklären mit einem grundlegend verschiedenen Verständnis der Rolle des Staates für das Alltagsleben der Bürger. In Deutschland kommt der sozialen Komponente der Marktwirtschaft eine bedeutende Stellung zu: Der Staat soll die Bedingungen für die Freiheit aller Bürger schaffen und dabei auch den Schutz der Schwachen sicherstellen. In der liberalen Tradition der Vereinigten Staaten liegt hingegen ein weitaus größerer Schwerpunkt darauf, durch einen freien Markt und ohne unnötige Einmischung des Staates das Leben gestalten zu können.

Für Deutschland ist daher die Beibehaltung und weitere Ausdifferenzierung der Schutzpflichten hinsichtlich der durch informationelle Preisgabe entstehenden Gefahren angebracht und dürfte auch den Wünschen der Bürger entsprechen. Eine schrittweise Anpassung der US-Rechtslage an die deutsche könnte, auch ohne Änderung des Verfassungstextes, dadurch erfolgen, dass die Gerichte verstärkt Anbieter von Dienstleistungen mit öffentlicher Relevanz, insbesondere Internet-Konzerne, als State Actors einstufen. Da diese in Bereichen tätig werden, in denen alternativ auch der Staat die Leistungen erbringen könnte, erscheint eine solche Bewertung nicht abwegig. Die Bürger sind typischerweise auf die privaten Unternehmen angewiesen, sodass von einer besonderen Schutzbedürftigkeit auszugehen ist.

Ein solcher Schritt würde zwar zu einem erhöhten Schutz der verfassungsmäßigen Rechte der Nutzer in den Vereinigten Staaten führen, erscheint jedoch angesichts der gefestigten Gerichtspraxis und der gesellschaftlichen Wirklichkeit derzeit als sehr unwahrscheinlich.

Kapitel 6

Rechtfertigung der Verhinderung der Preisgabe

Auch soweit der Staat zur Verhinderung informationeller Preisgabe im Internet nicht verpflichtet ist, kann der Erlass von diesbezüglichen Maßnahmen bei Vorliegen einer entsprechenden Rechtsgrundlage verfassungsrechtlich zumindest zulässig sein.

Im Folgenden sollen zunächst die Rechtslagen in Deutschland (siehe A) und den Vereinigten Staaten (siehe B) analysiert werden, bevor eine Gegenüberstellung beider erfolgt (siehe C).

A. Rechtfertigung nach dem Grundgesetz

Es bestehen Schutzpflichten zur Sicherung informationeller Selbstbestimmung, zur Verhinderung nicht selbstbestimmter Preisgabe sowie zur Verhinderung informationeller Preisgabe, die die Rechte Dritter verletzt.[1] Weiter stellt sich, auch soweit keine Schutzpflicht besteht, die Frage, ob Schutzmaßnahmen gerechtfertigt werden können.

Nachfolgend werden die Rechtfertigungsmöglichkeiten analysiert, wenn der Eingriff zum Schutz der selbstbestimmt Preisgebenden (siehe I), zum Schutz der nicht selbstbestimmt Preisgebenden (siehe II) sowie zum Schutz von Allgemeinwohlbelangen erfolgt (siehe III).

I. Rechtfertigung des Schutzes selbstbestimmt Preisgebender

Fraglich ist, ob der Staat diejenigen, die ihre informationelle Privatheit selbstbestimmt preisgeben wollen, vor sich selbst schützen darf. Eine staatliche Pflicht zum Schutz selbstbestimmt Preisgebender besteht jedenfalls, abgesehen von der Pflicht zur Sicherung der Selbstbestimmung, nicht.[2] Es könnte aber eine entsprechende Befugnis geben, wenn sich die Verhinderung der Preisgabe mit den Rechten der Preisgebenden und der verantwortlichen Stellen vereinbaren lässt.

---

[1] Siehe oben Kapitel 5,A.
[2] Siehe oben Kapitel 5,A.V.

1. Rechtfertigung hinsichtlich der Rechte der Preisgebenden

Ausgehend von der Untersuchung, ob Maßnahmen zur Verhinderung informationeller Preisgabe in das Recht auf informationelle Selbstbestimmung der Preisgebenden (siehe a)) sowie in weitere Rechte eingreifen (siehe b)), werden die gewonnenen Erkenntnisse auf die Fragen nach der Rechtfertigung zum Schutz der Preisgebenden vor sich selbst (siehe c)) und der Rechtfertigung zur Sicherung ihrer Selbstbestimmung (siehe d)) angewandt.

a) Evaluationsmaßstäbe zum Recht auf informationelle Selbstbestimmung

Zunächst könnte in das Recht auf informationelle Selbstbestimmung eingegriffen werden, wenn Nutzer an der Preisgabe ihrer Daten gehindert werden. Dafür müssten die Einbußen, die sie durch unterbleibende Preisgabe erlangen, vom Schutzbereich[3] dieses Rechts erfasst sein.

Informationelle Preisgabe dient zunächst dem Komfortgewinn im Alltagsleben. Dieses ist geprägt von einer Vielzahl kleiner Aufgaben und Entscheidungen. Zu ihrer Bewältigung sind die Einzelnen verstärkt von Online-Technologien abhängig, die, um funktionieren zu können, der Daten der Nutzer bedürfen. Die Analyse dieser personenbezogenen Daten im Rahmen von automatisierter Datenverarbeitung bietet Unterstützung. Sie filtert die Vielzahl an Möglichkeiten danach, welche aufgrund des Profils und bisherigen Verhaltens der Nutzer wahrscheinlich von ihnen gewollt sind. Voraussetzung für diese Analyse ist die vorherige Preisgabe der entsprechenden personenbezogenen Daten. Der Nutzen ist eine Entlastung im Alltagsleben. Obwohl ein praktisches Interesse an diesem Komfortgewinn besteht, findet dieses wenn überhaupt verfassungsrechtliche Absicherung durch das, vergleichsweise leicht einzuschränkende, Auffanggrundrecht der allgemeinen Handlungsfreiheit.

Das allgemeine Persönlichkeitsrecht gewährleistet allerdings positiv das Recht, auf die eigene Selbstdarstellung gezielt Einfluss zu nehmen.[4] Die Einzelnen sollen selbst darüber befinden können, wie sie sich gegenüber Dritten oder der Öffentlichkeit darstellen wollen, was ihren sozialen Geltungsanspruch ausmachen soll und ob oder inwieweit Dritte über ihre Persönlichkeit verfügen können, indem sie diese zum Gegenstand öffentlicher Erörterung machen.[5]

Eine Konsequenz dieses Bedürfnisses nach Kontrolle der Selbstdarstellung ist die Existenz des Rechts auf informationelle Selbstbestimmung. Dieses Recht umfasst die Befugnis, selbst zu entscheiden, wann und innerhalb welcher Grenzen man

---

[3] Generell zu Herleitung, Funktion und Schutzbereich des Rechts auf informationelle Selbstbestimmung: siehe oben Kapitel 3,B.I.1.

[4] BVerfGE 35, 202 (220); *Dreier*, in: ders. (Hrsg.), Grundgesetz-Kommentar I, 2013, 377, Art. 2 Abs. 1, Rn. 72.

[5] BVerfGE 63, 131 (142).

persönliche Sachverhalte offenbaren möchte.[6] Personen entfalten sich durch Interaktion mit anderen und haben in privaten wie geschäftlichen Beziehungen ein Interesse daran, sich in bestimmter Art und Weise darzustellen und so Einfluss zu nehmen auf die Vorstellungen, die Andere von ihnen gewinnen. Durch die Preisgabe bestimmter personenbezogener Daten können Eindrücke bei Anderen vermittelt und Reaktionen hervorgerufen werden. Die Offenlegung sensibler Daten kann auch genutzt werden, um gerade dadurch einer Diskriminierung zu entgehen. So kann es beispielsweise im Interesse von Männern mit Migrationshintergrund liegen, dass potenzielle Arbeitgeber leichten Zugriff auf ihr makelloses Vorstrafenregister erhalten. Andernfalls besteht die Gefahr, dass Arbeitgeber aufgrund der statistisch höheren Vorbestraftenrate von Männern mit Migrationshintergrund pauschal diskriminieren und Mitbewerber vorziehen.[7] Generell bietet das Internet den Nutzern die Möglichkeit, sich auch über große Distanzen hinweg selbst darzustellen. Die so mögliche Interaktion mit ihren Adressaten ermöglicht es ihnen, sich selbst zu entfalten und in der Gesellschaft zu platzieren.

Personenbezogenen Daten kommt zudem ein ökonomischer Wert zu. Nutzer geben im Internet personenbezogene Daten preis, die automatisiert verarbeitet werden, insbesondere zu Werbezwecken. Als Gegenleistung erhalten sie die Möglichkeit zur unentgeltlichen Nutzung von Angeboten. Diese reichen von E-Mail-Postfächern, sozialen Netzwerken, Cloud-Angeboten bis hin zu Foren oder Online-Inhalten von Zeitungen. Diese können sie zu privaten oder geschäftlichen Zwecken nutzen. Denkbare Alternative zu werbefinanzierten Internetangeboten sind entgeltliche Dienste. Diese können an sich privatheitsschonender sein, da sie nicht auf personalisierte Werbung als Einnahmequelle angewiesen sind. Zugleich können sie jedoch bewirken, dass finanziell prekär gestellte Nutzer auf sie verzichten. Dadurch kann Privatheit zur Klassenfrage werden, wenn der Staat nicht ein gewisses Privatheitsniveau garantiert.[8]

Gelegentlich werden die Ausführungen im Volkszählungsurteil als ein Appell für eine eigentumsähnliche Verfügungsmacht über personenbezogene Daten und daraus gewonnene Informationen verstanden.[9] Dieser, schon mit Wortlaut und Telos des Volkszählungsurteils nicht vereinbare Ansatz fand und findet jedoch klarstel-

[6] BVerfGE 65, 1 (42); 80, 367 (373); 85, 219 (224) und 96, 171 (181).

[7] *Strahilevitz*, Towards a Positive Theory of Privacy Law, 126 Harvard L. Rev. (2013), 2010, 2018 f.

[8] Dabei ist auch zu bedenken, dass Unternehmen ein größeres Interesse an den Daten reicher Nutzer haben können als an den Daten armer. Daher kann der Aufwand, den Unternehmen betreiben, um reiche Nutzer zur Preisgabe ihrer Daten zu bewegen, den um die Daten armer Nutzer betriebenen Aufwand übersteigen. Dies kann dazu führen, dass reichen Nutzern ein attraktiverer Service geboten wird als armen, wodurch letztere in doppelter Hinsicht verlieren: vgl.: *Cohen*, Examined Lives, 52 Stanford L. Rev. Online (2000), 1373, 1398; in diese Richtung auch: *Jerome*, Buying and Selling Privacy, 66 Stanford L. Rev. Online (2013), 47, 47 ff.

[9] *Künast*, „Meine Daten gehören mir" – und der Datenschutz gehört ins Grundgesetz, ZRP 2008, 201 ff.; ausführlich zum Konzept des Dateneigentums: *Buchner*, Informationelle Selbstbestimmung im Privatrecht, 2006; *ders.*, Eigentumsrechte an persönlichen Daten?, in: Redeker/Hop-

lende Gegenstimmen.[10] So sieht das Bundesverfassungsgericht schon im Volkszählungsurteil die Information als „Abbild sozialer Realität“, das „nicht ausschließlich dem Betroffenen allein zugeordnet werden kann“.[11] Das Recht auf informationelle Selbstbestimmung gewährt damit kein Eigentumsrecht an den Daten. Gerade als Ausfluss von Autonomie muss es aber angesichts der vielfältigen Einsetzbarkeit personenbezogener Daten das Recht beinhalten, diese nach eigener Kosten-Nutzen-Abwägung offenbaren zu können.[12] Die Preisgabe der eigenen Daten ist daher vom Schutzbereich des Rechts auf informationelle Selbstbestimmung umfasst.[13]

Zu klären ist, ob der Verhinderung der Preisgabe durch erzwungenen Schutz, durch die Unterstützung informationellen Selbstschutzes und durch Entscheidungsarchitekturen jeweils Eingriffscharakter zukommt:

Selbstgefährdendes Verhalten ist nicht als Grundrechtsverzicht[14] durch die Grundrechtsträger selbst zu klassifizieren. Vielmehr stellt das Nichtausschöpfen grundrechtlich geschützter Freiheiten ebenfalls eine Freiheitsausübung dar. Dies wird deutlich vor dem Hintergrund, dass die allgemeine Handlungsfreiheit (Art. 2 Abs. 1 GG) als Auffanggrundrecht und Komponente des Rechts auf informationelle Selbstbestimmung nicht nur den Persönlichkeitskern schützt, sondern jedes menschliche Verhalten.[15] Aus der Ablehnung der Persönlichkeitskerntheorie folgt, dass auch die Nichtinanspruchnahme grundrechtlich geschützter Freiheiten durch selbstschädigendes und -gefährdendes Verhalten in den Schutzbereich des Art. 2 Abs. 1 GG fällt.[16]

---

pen (Hrsg.), DGRI Jahrbuch 2011, 2012, 53 ff.; *Cohen*, Examined Lives, 52 Stanford L. Rev. Online (2000), 1373, 1377 ff.

[10] *Gurlit*, Verfassungsrechtliche Rahmenbedingungen des Datenschutzes, NJW 2010, 1035, 1036; *Podlech*, Aufgaben und Problematiken des Datenschutzes, 5 DVR (1976), 23, 28; *Simitis*, Die informationelle Selbstbestimmung, NJW 1984, 394, 400; *Trute*, Verfassungsrechtliche Grundlagen, in: Roßnagel (Hrsg.), Handbuch Datenschutzrecht, 2003, 156, 169, Rn. 21 f.; *Specht* will jedenfalls, wenn auch nicht ganz überzeugend, Lizenzen an materialisierten personenbezogenen Daten einräumen: *Specht*, Konsequenzen der Ökonomisierung informationeller Selbstbestimmung, in: Scholz/Funk (Hrsg.), DGRI Jahrbuch 2012, 2013, 239, 242 f.

[11] BVerfGE 1, 65 (44).

[12] Vgl.: *Weichert*, Die Ökonomisierung des Rechts auf informationelle Selbstbestimmung, NJW 2001, 1463, 1466 f.

[13] So auch: *Hansen*, Herausforderungen für den selbstbestimmten Bürger, in: Kompetenzzentrum Öffentliche IT (Hrsg.), Menschen in der digitalen Gesellschaft, 2014, 12; *Kutscha*, Erster Teil, in: Kutscha/Thomé (Hrsg.), Grundrechtsschutz im Internet?, 2013, 11, 47; *Schliesky/Hoffmann/Luch u. a.*, Schutzpflichten und Drittwirkung im Internet, 2014, 96 ff. stellen lediglich auf die allgemeine Handlungsfreiheit ab, betonen jedoch, dass deren Kern auf Art. 1 Abs. 1 GG zurückzuführen ist.

[14] Der Terminus „Grundrechtsverzicht“ bezieht sich nur auf das Verhältnis Bürger – Staat. Da Grundrechte nicht gegenüber Privaten gelten, kann ihnen gegenüber auch nicht auf Grundrechte verzichtet werden, vgl.: *Wietfeld*, Selbstbestimmung und Selbstverantwortung, 2012, 60 f.

[15] St. Rspr., seit: BVerfGE 6, 32 (36); bekräftigt durch: BVerfGE 80, 137 (152 ff.).

[16] *Hillgruber*, Der Schutz des Menschen vor sich selbst, 1992, 112 ff.; so mit ausführlicher Herleitung auch: *Fischer*, Die Zulässigkeit aufgedrängten staatlichen Schutzes vor Selbstschädigung, 1997, 75 ff., 84 f.

Wird die Grundrechtsausübung zum Schutz der Grundrechtsträger selbst verhindert, ist es präzise, von einem „Schutz durch Eingriff“ zu sprechen.[17] Nach dem klassischen Eingriffsbegriff ist jedes staatliche Verhalten, das final und unmittelbar die Grundrechte der Betroffenen beeinträchtigt und notfalls auch mit Befehl und Zwang durchgesetzt werden kann, ein Eingriff.[18] Es zeigte sich jedoch, dass Grundrechte auch durch Verhalten Privater berührt werden können, welches als Reaktion auf staatliches Handeln erfolgt. In Fortentwicklung des klassischen Verständnisses hat sich daher ein moderner, weitergehender Eingriffsbegriff durchgesetzt, der auch schlichtes Staatshandeln umfasst, das mittelbar-faktisch die Grundrechte der Betroffenen beeinträchtigt.[19]

Auch wenn Grundrechtsträger durch bloße Abschreckung von der Ausübung ihrer Grundrechte abgehalten werden, ohne dass sie konkret an der Ausübung gehindert würden, kann dies einen mittelbar-faktischen Grundrechtseingriff darstellen.[20] Das Hervorrufen gravierender Einschüchterungseffekte stellt einen Eingriff in das Recht auf informationelle Selbstbestimmung dar.[21] Auch erfasst sind heimliche Maßnahmen, da diese die Selbstdarstellungsmöglichkeit der Einzelnen ebenso beeinträchtigen wie offene Maßnahmen und die Nutzer zudem mangels Kenntnis des Eingriffs und der Person des Eingreifenden der Möglichkeit berauben, auf die entstehenden Fremdbilder Einfluss zu nehmen.[22] Die notwendige Erheblichkeit beruht auf dem Bewusstsein, aufgrund mangelnder Transparenz nie einschätzen zu können, ob die Grundrechtsträger gerade heimlicher staatlicher Intervention oder Überwachung ausgesetzt sind. Entsprechend ist der Grundrechtseingriff zeitlich nicht auf die Dauer der Intervention beschränkt, sondern währt fort, solange bei den Grundrechtsträgern Unsicherheit darüber besteht, ob sie Gegenstand eines Eingriffs sind.[23]

Ein erzwungener Schutz hat bereits nach dem klassischen Verständnis Eingriffscharakter. Auch können Entscheidungsarchitekturen nach dem modernen Eingriffsbegriff einen Eingriff darstellen, da sie durch Ausnutzung vorhersehbarer kognitiver Fehler der Preisgebenden die Grundrechtsausübung mittelbar-faktisch beeinträchtigen können.[24] Dagegen liegt in der Unterstützung informationellen

---

[17] Der Begriff wurde mit Blick auf den Eingriff in die Grundrechte störender Dritter geprägt durch: *Wahl/Masing*, Schutz durch Eingriff, JZ 1990, 553 ff.

[18] Zum klassischen Eingriffsbegriff und seinem Wandel: *Schoch*, Die Schwierigkeiten des BVerfG mit der Bewältigung staatlichen Informationshandelns, NVwZ 2011, 193 ff.

[19] Vgl.: BVerfGE 105, 252; 105, 279; ausführlich zum Konzept des faktischen Eingriffs: *Roth*, Faktische Eingriffe in Freiheit und Eigentum, 1994, 7 ff. und *Murswiek*, Das Bundesverfassungsgericht und die Dogmatik mittelbarer Grundrechtseingriffe, NVwZ 2003, 1, 2.

[20] *Oermann/Staben*, Mittelbare Grundrechtseingriffe durch Abschreckung, 52 Der Staat (2013), 630, 640 ff.

[21] Siehe oben Kapitel 3,B.I.1.a).

[22] *Schwabenbauer*, Heimliche Grundrechtseingriffe, 2013, 115 ff.

[23] Vgl.: *Oermann/Staben*, Mittelbare Grundrechtseingriffe durch Abschreckung, 52 Der Staat (2013), 630, 647.

[24] Sehr kritisch zu sehen und häufig vernachlässigt ist auch der Umstand, dass viele Maßnahmen der Entscheidungsarchitektur schon systemimmanent und kaum rechtfertigbar gegen das

Selbstschutzes kein Eingriff hinsichtlich der Rechte der Nutzer, da diesen lediglich zusätzliche Optionen geboten werden. Da die Maßnahmen zur Unterstützung informationellen Selbstschutzes lediglich Möglichkeiten eröffnen, ohne den Nutzern eine nennenswerte Belastung aufzuerlegen, verbleiben sie unterhalb der Eingriffsschwelle und bedürfen keiner Rechtfertigung.

Das Recht auf informationelle Selbstbestimmung ist nicht schrankenlos gewährleistet, vielmehr sind die Einzelnen sich innerhalb der sozialen Gemeinschaft entfaltende, auf Kommunikation angewiesene Persönlichkeiten und müssen Einschränkungen im überwiegenden Allgemeininteresse hinnehmen.[25] Diese Grenzen sind bedingt durch die vielseitige Einbindung der Grundrechtsträger in soziale Zusammenhänge, kurz: durch ihre grundsätzliche Gemeinschaftsbezogenheit und Gemeinschaftsgebundenheit.[26] Das informationelle Selbstbestimmungsrecht unterliegt – jedenfalls dem Grunde nach – der Schrankentrias des Art. 2 Abs. 1, 2. Halbsatz GG und ist damit zum Schutz von Rechten Anderer, der verfassungsmäßigen Ordnung oder des Sittengesetzes einschränkbar.[27] Angesichts des Menschenwürdekerns des Rechts auf informationelle Selbstbestimmung sind jedoch ergänzend erhöhte Anforderungen an die Verhältnismäßigkeitsprüfung zu stellen: Der durch die Menschenwürde geschützte Kernbereich privater Lebensgestaltung ist absolut geschützt.[28]

Eingriffe können auf gesetzlicher Grundlage unter Einhaltung des Verhältnismäßigkeitsgrundsatzes als Schranken-Schranke gerechtfertigt werden. Das eingesetzte Mittel muss geeignet, erforderlich und angemessen zur Erreichung eines legitimen Zwecks sein.[29]

Verfassungslegitime Zwecke lassen sich zunächst erkennen aus qualifizierten Schrankenvorbehalten, aus Grundrechten, aus verfassungsrechtlich statuierten Ge-

---

Recht auf informationelle Selbstbestimmung der Betroffenen verstoßen: Dies ist immer dann der Fall, wenn die Präferenzen der Betroffenen erst unter Verletzung ihrer informationellen Privatheit ermittelt werden können, um sie dann in einem zweiten Schritt durch Entscheidungsarchitektur zur Wahrung ihrer informationellen Privatheit gemäß den ermittelten Präferenzen zu bewegen. Zu diesem, hier nicht weiter ausgeführten Aspekt, siehe die Kritik von: *Kapsner/Sandfuchs*, Nudging as a Threat to Privacy, 6 Rev. of Philosophy and Psychology (2015), 455 ff. sowie die Stellungnahme von *Sunstein*, Nudges, Agency, and Abstraction, 6 Rev. of Philosophy and Psychology (2015), 511, 526 „Kapsner and Sandfuchs (…) argue convincingly that to know how to nudge, choice architects might have to assemble a great deal of information, some of which people might want to keep private. If public officials are designing default rules that could compromise privacy, they should want to know whether the affected people (as individuals) care about privacy or not. For those who do care, such officials might adopt privacy-protective defaults; for those who do not, they might not. So far, perhaps, so good. But Kapsner and Sandfuchs make a clever (and to my knowledge original) objection, which is that *people might not even want government to know whether they care about privacy*. (…)" (Hervorhebung im Original).

[25] BVerfGE 65, 1 (44).

[26] BVerfGE 65, 1 (44) (m.w.N.).

[27] Das Bundesverfassungsgericht orientiert sich „zumindest verbal" an der Schrankentrias: *Dreier*, in: ders. (Hrsg.), Grundgesetz-Kommentar I, 2013, Art. 2 Abs. 1, Rn. 91.

[28] BVerfGE 120, 274 (335); *Rudolf*, Recht auf informationelle Selbstbestimmung, in: Merten/Papier (Hrsg.), Handbuch der Grundrechte in Deutschland und Europa IV, 2011, 233, 286, Rn. 85.

[29] St. Rspr., statt vieler: BVerfGE 17, 306 (314).

setzgebungsaufträgen, aus Staatszielbestimmungen, aus grundgesetzlichen Kompetenzbestimmungen sowie aus Staatsfundamentalbestimmungen, wie dem Rechtsstaatlichkeitsprinzip.[30] Fraglich ist jedoch, ob auch Zwecke als legitim betrachtet werden können, die keinen Niederschlag im Grundgesetz gefunden haben. Nach wohl herrschendem Verständnis ist ein Zweck legitim, wenn ihm sachgerechte und vernünftige Erwägungen des Gemeinwohls zugrunde liegen, die der Wertordnung des Grundgesetzes nicht widersprechen.[31] Seitens des Bundesverfassungsgerichts wird entsprechend teilweise die Verfolgung jedes öffentlichen Interesses als zulässige Eingriffsrechtfertigung gesehen. So führt es im Handwerksordnungs-Beschluss aus, dem Gesetzgeber stehe es frei, auch Gemeinschaftsinteressen zum Eingriffsanlass zu nehmen, die sich erst aus seinen besonderen wirtschafts-, sozial- und gesellschaftspolitischen Vorstellungen und Zielen ergeben und die er also erst selbst in den Rang wichtiger Gemeinschaftsinteressen erhebt.[32] Einschränkender äußert es sich im Beschluss zum Familiennachzug, wonach das Grundgesetz es nicht ausschließe, den Schutz von Grundrechtsgütern zugunsten anderer nicht verfassungsrangiger Belange in bestimmtem Umfang zurückzustellen.[33]

Andere Stimmen lehnen eine derart weite Auslegung ab und lassen de facto Grundrechtseinschränkungen nur zum Zweck des Schutzes von Interessen zu, die ebenfalls mit Verfassungsrang ausgestattet sind.[34] In diese Richtung lässt sich auch die Spiegel-Entscheidung des Bundesverfassungsgerichts lesen, wonach die Pressefreiheit die Möglichkeit in sich berge, mit anderen vom Grundgesetz geschützten Werten in Konflikt zu geraten.[35]

Die letztgenannte Auffassung erscheint im Ergebnis vorzugswürdig. Zwar ist dem Bundesverfassungsgericht zuzustimmen, dass der Staat im Rahmen seiner Einschätzungsprärogative die Eingriffszwecke frei wählen kann. Doch wird ein nicht mit Verfassungsrang ausgestattetes Interesse in der Verhältnismäßigkeitsabwägung qua Automatismus gegenüber dem eingeschränkten Grundrecht unterliegen.[36] Eine gleichberechtigte Interessenabwägung setzt die prinzipielle Gleichrangigkeit der Interessen voraus. Nicht verfassungsrechtlich geschützte Interessen sind

---

[30] *Merten*, Verhältnismäßigkeitsgrundsatz, in: Merten/Papier (Hrsg.), Handbuch der Grundrechte in Deutschland und Europa III, 2009, 517, 550 f., Rn. 59 ff.

[31] BVerfGE 30, 292 (316); *Isensee*, Das Grundrecht als Abwehrrecht und als staatliche Schutzpflicht, in: Isensee/Kirchhof (Hrsg.), Handbuch des Staatsrechts der Bundesrepublik Deutschland X, 2012, 413, 475, Rn. 13 und *Merten*, Verhältnismäßigkeitsgrundsatz, in: Merten/Papier (Hrsg.), Handbuch der Grundrechte in Deutschland und Europa III, 2009, 517, 551 f., Rn. 62.

[32] BVerfGE 13, 97, 107.

[33] BVerfGE 76, 1, 53.

[34] *Doehring*, Die Gesunderhaltung des Menschen im Spannungsverhältnis zwischen Staatsfürsorge und Individualentscheidung, in: Fürst/Herzog/Umbach (Hrsg.), Festschrift für Wolfgang Zeidler Band II, 1987, 1553, 1555 und *Fischer*, Die Zulässigkeit aufgedrängten staatlichen Schutzes vor Selbstschädigung, 1997, 133 ff.

[35] BVerfGE 20, 162, 176.

[36] So auch: *Fischer*, Die Zulässigkeit aufgedrängten staatlichen Schutzes vor Selbstschädigung, 1997, 140 ff.

nicht gleichrangig mit den eingeschränkten Grundrechten und können daher nicht zur Eingriffsrechtfertigung herangezogen werden. Es erscheint verfehlt, Interessen zum legitimen Eingriffszweck zu erheben, wenn sie im Rahmen der Verhältnismäßigkeitsprüfung immer unterliegen werden. Will man das Kriterium des „legitimen Zwecks" nicht zur Farce verkommen lassen, können nur solche Zwecke als legitim gelten, die jedenfalls irgendwie gearteten Verfassungsbezug aufweisen.[37] Der erforderliche Verfassungsbezug des gesetzgeberischen Zweckes soll vorliegen, wenn der Eingriff nicht Selbstzweck ist, sondern einem Rechtsprinzip dient.[38] Dies sei der Fall, wenn ein Verfassungsprinzip so weit konkretisiert werden kann, dass der Zweck zumindest ein „Partikel dieses Prinzips" darstellt.[39] Dadurch, dass der in Rede stehende Eingriff nicht erfolgt, müsse ein anderes Verfassungsprinzip eine Einbuße in seinem Wirkungsgehalt gegenüber dem Zustand erleiden, der bestünde, wenn der Eingriff erfolgt wäre.[40] Diese Herangehensweise überzeugt, da sie den Zweck des Eingriffs in sinnvollem Maße rückbezieht auf ein durch die Verfassung geschütztes Recht. Nicht erforderlich ist hingegen, dass das Grundgesetz ausdrücklichen Schutz vor exakt den befürchteten Bedrohungen bietet. Die Erfüllung einer Schutzpflicht ist jedenfalls ein legitimer Zweck.[41]

Geeignet ist ein Mittel nach überwiegender Meinung, wenn mit seiner Hilfe der gewünschte Zweck zumindest gefördert werden kann.[42] Bei der Einschätzung der Geeignetheit kommt dem Gesetzgeber ein Einschätzungsspielraum zu, der von der Eigenart des in Rede stehenden Sachbereichs, den Möglichkeiten, sich ein hinreichend sicheres Urteil zu bilden und der Bedeutung der auf dem Spiel stehenden Rechtsgüter beeinflusst wird.[43] Dabei sei nach der dominierenden Ansicht nicht zu fordern, dass stets oder auch nur im Regelfall von dem Erfolg der Maßnahme auszugehen sei.[44] Unschädlich sei, dass die Maßnahme nur in vergleichsweise wenigen Fällen Erkenntnisse verspreche.[45] Ausreichend sei die abstrakte Möglichkeit der Zweckerreichung.[46] Die derart weite Interpretation des Geeignetheitsbegriffs lässt die Geeignetheit als eigene Stufe der Verhältnismäßigkeitsprüfung jedoch weitest-

---

[37] Unbenommen bleibt es dem Gesetzgeber jedoch, durch offene Formulierung seiner Handlungsziele den erforderlichen Verfassungsbezug herzustellen.

[38] *Fischer*, Die Zulässigkeit aufgedrängten staatlichen Schutzes vor Selbstschädigung, 1997, 134.

[39] *Fischer*, Die Zulässigkeit aufgedrängten staatlichen Schutzes vor Selbstschädigung, 1997, 147.

[40] *Fischer*, Die Zulässigkeit aufgedrängten staatlichen Schutzes vor Selbstschädigung, 1997, 147.

[41] *Isensee*, Das Grundrecht als Abwehrrecht und als staatliche Schutzpflicht, in: Isensee/Kirchhof (Hrsg.), Handbuch des Staatsrechts der Bundesrepublik Deutschland X, 2012, 413, 475, Rn. 134.

[42] St. Rspr., statt vieler: BVerfGE 30, 292 (316).

[43] St. Rspr., statt vieler: BVerfGE 109, 279 (336).

[44] BVerfGE 120, 274 (320).

[45] BVerfGE 100, 313 (373) und 115, 320 (345) (für die Rasterfahndung).

[46] BVerfGE 100, 313 (373).

gehend leerlaufen. Einwände, eine Maßnahme sei überwiegend nicht zweckfördernd, werden auf die Stufe der Angemessenheitsprüfung gedrängt und dort nur als ein Aspekt unter vielen eingestellt.[47]

Diese Vorgehensweise überzeugt nicht.[48] Wenn jeder staatliche Eingriff in ein Grundrecht der Rechtfertigung bedarf, muss es dem Staat obliegen, den Beweis zu erbringen, dass das eingesetzte Mittel mehr als nur hypothetisch geeignet ist, den erwünschten Zweck zu erreichen. In diesem Sinne ist jedenfalls das Bestehen des vom Bundesverfassungsgericht in der Entscheidung zum Impfstoffversand hinsichtlich Art. 12 GG postulierten nachvollziehbaren Wirkungszusammenhangs zwischen Zweck und Mittel zu fordern.[49] Soweit eine derartige Einschätzung vorab nicht abgegeben werden kann, bedarf es einer effektiven Evaluierung.[50] In diesem Sinne führt das Bundesverfassungsgericht, wenn auch nur zur Berichtspflicht nach Art. 13 Abs. 6 GG, aus, die verbleibende Unsicherheit mache es erforderlich, die Entwicklung zu beobachten und fortlaufend zu prüfen, ob das Ermittlungsinstrument tatsächlich geeignet ist, auch das mit ihm verfolgte spezielle Ziel in hinreichendem Maße zu erreichen.[51]

Weiter ist die Erforderlichkeit gegeben, wenn der Gesetzgeber kein gleich wirksames, aber das Grundrecht nicht oder weniger fühlbar einschränkendes Mittel wählen kann.[52]

Die Angemessenheit ist schließlich zu bejahen, wenn die Beeinträchtigung bei einer Gesamtbetrachtung nicht außer Verhältnis zum Zweck steht und den Betroffenen zumutbar ist.[53] Es ist zu berücksichtigen, dass staatliche Maßnahmen weniger einschneidend sind, wenn sie informationelle Preisgabe nur limitieren, anstatt sie zu verhindern. Zu gelten hat das Prinzip des „schonendsten Paternalismus“.[54] Die Unterstützung informationellen Selbstschutzes ist in dieser Hinsicht damit regelmäßig

---

[47] Eine vergleichbare Problematik stellt sich zudem im Rahmen der Erforderlichkeits-Prüfung, der in der Gerichtspraxis ebenso wie der Geeignetheits-Prüfung eine nur sehr untergeordnete Bedeutung zukommt. Dies wird insbesondere, wie im Fall der Vorratsdatenspeicherung, virulent, wenn zu einem sehr weiten Zweck umfassende Datenerhebungen stattfinden. In diesen Fällen wird die Maßnahme den Zweck immer irgendwie fördern können (Geeignetheit) und weniger umfassende Mittel werden immer jedenfalls etwas weniger wirksam sein als das umfassende (Erforderlichkeit). Problematisch ist dies, da es in der Hand des Gesetzgebers liegt, Zweck und Maßnahme beliebig weit zu fassen, siehe dazu: *Hornung*, Datenschutz, PVS Sonderheft 46, 2012, 377, 391 ff.

[48] So auch: *Schwabenbauer*, Heimliche Grundrechtseingriffe, 2013, 208.

[49] BVerfGE 107, 186 (197).

[50] *Schwabenbauer*, Heimliche Grundrechtseingriffe, 2013, 209, 358 ff.

[51] BVerfGE 109, 279 (340); später ausgebaut in BVerfGE 112, 304 (320 f.), dazu: *Hornung*, Die kumulative Wirkung von Überwachungsmaßnahmen, in: Albers/Weinzierl (Hrsg.), Menschenrechtliche Standards in der Sicherheitspolitik, 2010, 65, 66 ff.

[52] St. Rspr., statt vieler: BVerfGE 25, 1 (18); zur Problematik im Fall von Informationseingriffen mit großer Streubreite: *Hornung*, Datenschutz PVS Sonderheft 46, 2012, 377 ff.

[53] *Nußberger*, Das Verhältnismäßigkeitsprinzip als Strukturprinzip richterlichen Entscheidens in Europa, NVwZ-Beilage 2013, 36, 40.

[54] *Van Aaken*, Begrenzte Rationalität und Paternalismusgefahr, in: Anderheiden/Bürkli/Heinig u. a. (Hrsg.), Paternalismus und Recht, 2006, 109, 133.

ein milderes Mittel als Entscheidungsarchitekturen; Letztere sind wiederum ein milderes Mittel als die Anwendung von erzwungenem Schutz. Mit dieser Einschätzung ist jedoch Vorsicht geboten. Unter der Prämisse, dass Individuen tatsächlich so stark durch Entscheidungsarchitekturen beeinflusst werden können, wie die Verhaltensökonomie annimmt, ist es unwahrscheinlich, dass sie sich entgegen der durch die Entscheidungsarchitekturen anvisierten Richtung entschließen.[55] Entscheidungsarchitekturen nähern sich erzwungenem Schutz daher an.[56]

Erzwungener Schutz und der Einsatz von Entscheidungsarchitekturen stellen einen Eingriff in das Recht auf informationelle Selbstbestimmung der Preisgebenden dar und bedürfen der dargestellten verfassungsrechtlichen Rechtfertigung.

b) *Evaluationsmaßstäbe zu anderen möglicherweise beeinträchtigten Rechten*

Neben dem Recht auf informationelle Selbstbestimmung kann durch die Verhinderung informationeller Preisgabe auch in andere Grundrechte eingegriffen werden.

Denkbar wäre, dass die Verhinderung informationeller Preisgabe auch einen Eingriff in die Informationsfreiheit (Art. 5 Abs. 1 Satz 1, Halbsatz 2 GG) der Preisgebenden darstellt. In diese Richtung kann argumentiert werden, informationelle Preisgabe erleichtere die personalisierte Versorgung mit Informationen und unterstütze so den Zugang zu Informationen. Der Ansatz, durch die Verhinderung informationeller Preisgabe würde in die Informationsfreiheit eingegriffen, ist jedoch nicht weiterführend. Die Informationsfreiheit schützt die Nutzer davor, dass sie der Staat vom ungehinderten Zugang zu Informationen abhält. Die hier gegenständlichen staatlichen Maßnahmen zur Verhinderung informationeller Preisgabe verhindern gerade nicht den ungehinderten Zugang zu Informationen, sondern unterbinden lediglich, dass der Informationsauswahlprozess beeinflusst wird, wodurch wiederum der ungehinderte Zugang zu Informationen sichergestellt werden soll. Es ist daher vorzugswürdig, Maßnahmen zur Verhinderung informationeller Preisgabe im Regelfall nicht an der Informationsfreiheit zu messen.

Weiter könnte die Verhinderung informationeller Preisgabe in die Meinungsfreiheit (Art. 5 Abs. 1 Satz 1, Halbsatz 1 GG) eingreifen. Eine Meinung ist gekennzeichnet durch ein „Element der Stellungnahme, des Dafürhaltens, des Meinens im Rahmen einer geistigen Auseinandersetzung".[57] Die vorliegende Untersuchung befasst sich mit der Preisgabe eigener personenbezogener Daten, sodass regelmäßig keine Meinungsäußerung gegeben sein wird. Etwas anderes gilt jedoch in den Fällen, in denen die Meinungsäußerung direkt und notwendigerweise mit der Preisgabe personenbezogener Daten verbunden wird.[58]

---

[55] *Mitchell*, Libertarian Paternalism Is an Oxymoron, 5.2002 FSU College of Law, Law and Economics Paper, 1, 12.

[56] Vgl.: *Mitchell*, Libertarian Paternalism Is an Oxymoron, 5.2002 FSU College of Law, Law and Economics Paper, 1, 12.

[57] St. Rspr., BVerfGE 61, 1 (8).

[58] Ein solcher Falle läge beispielsweise vor, wenn es im Rahmen einer politischen Meinungsäu-

Soweit, abhängig von der Fallgestaltung, die Informations- oder Meinungsfreiheit doch einschlägig ist, können Eingriffe gerechtfertigt werden auf Basis allgemeiner Gesetze, gesetzlicher Bestimmungen zum Schutz der Jugend und des Rechts der persönlichen Ehre (Art. 5 Abs. 2 GG). Praktische Bedeutung liegt auf der Schranke der allgemeinen Gesetze. Allgemein ist ein Gesetz, wenn es nicht eine Meinung als solche verbietet, sich nicht gegen die Äußerung der Meinung als solche richtet, sondern vielmehr dem Schutz eines schlechthin ohne Rücksicht auf eine bestimmte Meinung zu schützenden Rechtsguts dient.[59] Das Rechtsgut muss in der Rechtsordnung allgemein und unabhängig davon geschützt sein, ob es durch Meinungsäußerungen oder auf andere Weise verletzt werden kann.[60] Zudem müssten die Schranken-Schranken beachtet werden. Es gilt die Wechselwirkungslehre, wonach das grundrechtsbeschränkende Gesetz im Lichte des beschränkten Grundrechts auszulegen ist.[61]

Schließlich kann die Verhinderung informationeller Preisgabe auch an der Berufsfreiheit (Art. 12 Abs. 1 GG) zu messen sein. Dafür muss die in Rede stehende Preisgabe im Zusammenhang stehen mit einer auf Dauer angelegten Tätigkeit, die der Schaffung und Erhaltung einer Lebensgrundlage dient.[62] Im Regelfall werden die in der vorliegenden Arbeit behandelten Preisgaben nicht in diese Kategorie fallen, sondern vielmehr an das persönliche Umfeld gerichtet sein. Soweit jedoch die Berufsfreiheit betroffen ist, ist die Schranke des Art. 12 Abs. 1 Satz 2 GG zu beachten.

c) Rechtfertigung des Schutzes vor sich selbst

Zu prüfen ist, ob die Verhinderung informationeller Preisgabe durch erzwungenen Schutz oder Entscheidungsarchitekturen mit den Rechten der Preisgebenden vereinbar ist, wenn diese Maßnahmen ausschließlich dem Zweck dienen, selbstbestimmt Preisgebende vor sich selbst zu schützen.

Die Verhinderung informationeller Preisgabe kann gerechtfertigt werden, wenn sie auf gesetzlicher Grundlage erfolgt und der Eingriff zur Erreichung eines legitimen Zwecks nicht unverhältnismäßig in die Rechte der Preisgebenden eingreift.

Ausschlaggebend ist, ob der Schutz der Preisgebenden vor der Gefährdung durch sich selbst einen legitimen Zweck darstellt. Der erforderliche Verfassungsbezug des gesetzgeberischen Zweckes liegt vor, wenn der Eingriff nicht Selbstzweck ist, sondern einem Rechtsprinzip dient.[63] Dafür muss ein Verfassungsprinzip so weit kon-

ßerung dezidiert darauf ankommt, dass diese den Preisgebenden zugeordnet werden kann, etwa, weil sie eine besondere gesellschaftliche Stellung innehaben.

[59] St. Rspr., seit: BVerfGE 7, 198 (209).

[60] BVerfGE 111, 147 (155).

[61] St. Rspr., seit: BVerfGE 7, 198 (208 f.).

[62] So die st. Rspr., vgl. :BVerfGE 7, 377 (397).

[63] Zu den an den legitimen Zweck zu stellenden Anforderungen, siehe oben: Kapitel 6,A.I.1.a); *Fischer*, Die Zulässigkeit aufgedrängten staatlichen Schutzes vor Selbstschädigung, 1997, 134.

kretisiert werden können, dass der Zweck zumindest ein „Partikel dieses Prinzips" darstellt.[64] Es ist daher zu untersuchen, ob der Schutz selbstbestimmt Handelnder vor sich selbst jedenfalls ein „Partikel" eines durch das Grundgesetz geschützten Prinzips ausmacht. Es müsste also ein grundrechtliches Prinzip geben, das den Schutz derjenigen, die sich selbstbestimmt gefährden, rechtfertigt.

Teilweise wird die Rechtfertigungsmöglichkeit staatlicher Maßnahmen zum Schutz der selbstbestimmt Handelnden vor sich selbst bejaht:[65] Das Bundesverfassungsgericht sieht in der viel kritisierten Entscheidung zur Lebendorganspende ohne weitere Begründung das Ziel, Menschen davor zu bewahren, sich selbst einen größeren persönlichen Schaden zuzufügen, als legitimes Gemeinwohlanliegen an, das den Schutz vor sich selbst rechtfertigen kann.[66] Auch stuft es wegen des hohen Rangs der zu schützenden Rechtsgüter Rauchverbote in Kleingastronomien, in denen sich nur die selbstständigen Wirte und freiwillige Gäste aufhalten, als verfassungsmäßig ein.[67]

In der Literatur wird ausgeführt, die Bürger hätten ihrerseits ein Interesse daran, sich auf das in der Gemeinschaft lebendige Sittengesetz verwiesen zu sehen, da es ihnen den Weg freigäbe für die Entfaltung ihres Personseins.[68] Menschen bedürften des Sittengesetzes, „um von hier aus zu schöpferischem Tun und eigener Wertverwirklichung durchstoßen zu können." Erst durch diese „Werterkenntnis und Wertschöpfung" würden sie zum Menschen. Die Rechtfertigung von Freiheitsbeschränkungen zum Schutz vor sich selbst wird unter anderem ausgedehnt auf den Impfzwang,[69] die Bekämpfung von Geschlechtskrankheiten[70] und die Bekämpfung gemeingefährlicher Krankheiten,[71] ohne dass dabei der, durch solche Maßnahmen wohl auch erreichte, Schutz Dritter in den Blick genommen wird.

Überzeugender ist es jedoch, den Schutz selbstbestimmt Preisgebender vor sich selbst nicht als legitimen Zweck einzustufen, sodass die mit ihm verbundenen Eingriffe nicht zu rechtfertigen sind:

---

64 *Fischer*, Die Zulässigkeit aufgedrängten staatlichen Schutzes vor Selbstschädigung, 1997, 147.

65 Nicht immer wird dabei deutlich unterschieden zwischen der Frage, ob der Staat verpflichtet ist, die Bürger vor sich selbst zu schützen (siehe oben Kapitel 5,A.V) und der hier diskutierten Frage, ob ein entsprechender Eingriff gerechtfertigt werden kann.

66 BVerfG NJW 1999, 3399, 3400; ablehnend: *Gutmann*, Gesetzgeberischer Paternalismus ohne Grenzen?, NJW 1999, 3387 ff.; *Kirste*, Harter und weicher Rechtspaternalismus, JZ 2011, 805, 811 und *Schroth*, Die Begrenzung des Spenderkreises im Transplantationsgesetz als Problem der paternalistischen Einschränkung menschlicher Freiheit, in: Schünemann/Müller/Philipps (Hrsg.), Das Menschenbild im weltweiten Wandel der Grundrechte, 2002, 35, 49 ff.

67 BVerfGE 121, 317 (357 f.).

68 Zu den folgenden Ausführungen, soweit nicht anders angegeben: *Häberle*, Die Wesensgehaltgarantie des Artikel 19 Abs. 2 Grundgesetz, [3]1983, 28 f.

69 Unter Bezug auf die zwischenzeitlich aufgehobene Entscheidung: BVerwGE 9, 78.

70 Unter Bezug auf das am 1.1.2001 außer Kraft getretene Gesetz über die Bekämpfung von Geschlechtskrankheiten (BGBl. I, 1953, 700).

71 Unter Bezug auf das Gesetz, betreffend die Bekämpfung gemeingefährlicher Krankheiten (RGBl. I, 1900, 306).

Das Bundesverfassungsgericht führt in seinem Urteil zur Jugendhilfe aus, dass staatliche Eingriffe mit dem alleinigen Ziel, die Betroffenen zu „bessern“, unzulässig sind.[72] Diese Einschätzung wird bekräftigt in dem Beschluss zur Verfassungsmäßigkeit von § 26 Bundessozialhilfegesetz.[73]

Auch anderorts in der Rechtsprechung wird der Schutz von sich selbstbestimmt Gefährdenden nur um ihrer selbst willen abgelehnt. In seinem Urteil zu den Tauchverboten führt der Verwaltungsgerichtshof Baden-Württemberg sogar aus, „ein Recht des Staates, den einzelnen Bürger an ihn ausschließlich selbst gefährdenden Unternehmungen zu hindern, wird […] heute, soweit ersichtlich, einhellig verneint.“[74]

Diese aus den letztgenannten Entscheidungen erkennbare freiheitsfokussierte Herangehensweise wird in der Literatur geteilt.[75] Die Individuen sind autonome Wesen und dürfen grundsätzlich frei verfahren. Eingeschlossen sei auch das Recht, objektiv falsche Alternativen zu wählen[76] und sich selbst zu gefährden und zu schädigen, selbst wenn dies zum eigenen Tod führe.[77] Entsprechend sei auch die freiwillige Datenpreisgabe in sozialen Netzwerken erfasst.[78] Andernfalls drohe unter dem Deckmantel des wohlmeinenden Paternalismus eine diktatorische Bevormundung der Einzelnen und somit die Erosion privater Freiräume.[79]

Teilweise wird eine Selbstgefährdung der Grundrechtsträger zugelassen, solange das in Rede stehende Handeln Ausdruck der Persönlichkeit und Selbstbestimmung der Grundrechtsträger ist. Träte dieser Aspekt in den Hintergrund, wie im Beispiel des Folter- oder Todesstrafeverbots, sei ein Verzicht ausgeschlossen.[80]

Eine tatbestandliche Pflicht zur Grundrechtsausübung oder zur Bewahrung der eigenen grundrechtlichen Freiheiten besteht nicht, abgesehen von Art. 6 Abs. 2 Satz 1

---

[72] BVerfGE 22, 180 (219 f.).

[73] BVerfGE 30, 47 (53).

[74] VGH Baden-Württemberg NJW 1998, 2235, 2236. Gegenstand des Verfahrens war ein Verbot, an einer besonders gefährlichen Stelle tauchen zu gehen. Dieses konnte nicht mit Blick auf den Schutz der sich Selbstgefährdenden gerechtfertigt werden, aber zum Schutz unbeteiligter Dritter, die durch einen Unfall zu gefährlichen Rettungsaktionen veranlasst werden könnten.

[75] Einen Überblick über die in Rechtsprechung und Literatur angeführten Argumente liefert *Wietfeld*. Dabei kommt er zu dem hier geteilten Schluss, dass der Schutz selbstbestimmt Handelnder vor sich selbst keinen legitimen Eingriffszweck darstellt: *Wietfeld*, Selbstbestimmung und Selbstverantwortung, 2012, 78 ff., insbesondere 81.

[76] Maunz/Dürig-GG/*Di Fabio*, 2014, Art. 2, Rn. 50 f. m. w. N. und *Littwin*, Grundrechtsschutz gegen sich selbst, 1993, 243.

[77] *Bernert-Auerbach*, Das Recht auf den eigenen Tod und aktive Sterbehilfe unter verfassungsrechtlichen Gesichtspunkten, 2012, 239 ff. und *Wietfeld*, Selbstbestimmung und Selbstverantwortung, 2012, 68 ff.

[78] *Gurlit*, Verfassungsrechtliche Rahmenbedingungen des Datenschutzes, NJW 2010, 1035, 1041.

[79] *Eidenmüller*, Effizienz als Rechtsprinzip, 1995, 390.

[80] *Schliesky/Hoffmann/Luch u. a.*, Schutzpflichten und Drittwirkung im Internet, 2014, 136. Dieses Beispiel ist jedoch dahingehend zu relativieren, dass Folter und Todesstrafe insbesondere von staatlicher Seite drohen könnten, während sich die vorliegende Arbeit auf Bedrohungen grundrechtlich geschützter Interessen durch Private fokussiert.

GG, der diese ausdrücklich normiert („Pflege und Erziehung der Kinder sind das natürliche Recht der Eltern und die zuvörderst ihnen obliegende Pflicht.").[81] Solche Pflichten lassen sich auch nicht annehmen, indem man Grundrechte als dienende Freiheiten konstruiert, die als Instrument zur Erreichung objektiver Zwecke fungieren.[82] Auch soweit die Unveräußerlichkeit von Grundrechten im Grundsatz anerkannt wird, geschieht dies nicht zum Schutz der selbstbestimmten Grundrechtsträger vor sich selbst, sondern zum Schutz vor fehlender Selbstbestimmung oder zum Schutz von Allgemeinwohlbelangen.[83] Grundrechte unterliegen auch keiner funktionalen inneren Schranke, nach der ihr Gebrauch schon tatbestandlich nur zulässig wäre, soweit es dem Erhalt der freiheitlich-demokratischen Grundordnung dient.[84]

Die Wahrnehmung der eigenen Grundrechte und der individuell als gültig angesehenen Werte unterliegt gerade nicht der staatlichen Kontrolle, sondern ist Teil der individuellen Freiheitsentfaltung. Dem würde es widersprechen, Freiheitseingriffe mit dem Zweck zu rechtfertigen, die Persönlichkeitsentwicklung zu unterstützen. Beeinträchtigungen von grundrechtlich geschützten Interessen, die von selbstbestimmt handelnden Grundrechtsträgern ausgehen, darf der Staat daher nicht allein aus diesem Grund abwehren. Die Rede ist von „aufgedrängtem Grundrechtsschutz" und womöglich der „Pervertierung der grundrechtlichen Freiheitsidee".[85] Schutz darf nicht „zur Bewachung ausarten".[86] Das Wohl des selbstbestimmt handelnden Menschen allein kann nicht als Rechtfertigung dienen.[87]

Auch das Recht auf informationelle Selbstbestimmung beinhaltet daher die Freiheit, Privatheit nicht in Anspruch zu nehmen.[88] Wie das Bundesverfassungsgericht feststellt, obliegt es den Einzelnen, ihre Kommunikationsbeziehungen zu gestalten und in diesem Rahmen darüber zu entscheiden, ob sie bestimmte Informationen preisgeben oder zurückhalten. „Die Freiheit der Privatautonomie beim Datenschutz beinhaltet also grundsätzlich die Möglichkeit eines ‚Paktes mit dem Teufel'".[89]

---

[81] *Bethge*, Grundpflichten als verfassungsrechtliche Dimension, NJW 1982, 2145, 2147 f.; *Höfling*, Menschenwürde und gute Sitten, NJW 1983, 1582, 1584 f.; *Kirste*, Harter und weicher Rechtspaternalismus, JZ 2011, 805, 811 f. und *Littwin*, Grundrechtsschutz gegen sich selbst, 1993, 109 ff. m. w. N.

[82] *Klein*, Die Grundrechtliche Schutzpflicht, DVBl. 1994, 489, 494 m. w. N.

[83] *Fisahn*, Ein unveräußerliches Grundrecht am eigenen genetischen, Code ZRP 2001, 49, 53 f.

[84] Ausführlich: *Littwin*, Grundrechtsschutz gegen sich selbst, 1993, 153 ff.

[85] *Dietlein*, Die Lehre von den grundrechtlichen Schutzpflichten, 1992; Eine „Pervertierung der Grundrechte" fürchtet auch: *Schwabe*, Der Schutz des Menschen vor sich selbst, JZ 1998, 66, 70.

[86] *Isensee*, Das Grundrecht auf Sicherheit, 1983, 48.

[87] So auch: *van Aaken*, Begrenzte Rationalität und Paternalismusgefahr, in: Anderheiden/Bürkli/Heinig u. a. (Hrsg.), Paternalismus und Recht, 2006, 109, 136; *Fischer*, Die Zulässigkeit aufgedrängten staatlichen Schutzes vor Selbstschädigung, 1997, 107 ff. m. w. N.; *Lange*, Grundrechtsbindung des Gesetzgebers, 2010, 397, Fn. 1; *Mill*, Über die Freiheit, 2010 (Original: 1859), 19 und *Schwabe*, Der Schutz des Menschen vor sich selbst, JZ 1998, 66, 66, 69 f.

[88] So auch: *Bull*, Persönlichkeitsschutz im Internet, NVwZ 2011, 257, 258 und *Masing*, Herausforderungen des Datenschutzes, NJW 2012, 2305, 2308.

[89] *Weichert*, Datenschutz als Verbraucherschutz, in: Peissl (Hrsg.), Privacy, 2003, 145, 150.

Folglich ist ein Einwilligungsverbot jedenfalls bei freiwilliger, informierter und jederzeit widerruflicher Einwilligung abzulehnen.[90] Geben Nutzer freiwillig ihre Daten preis, darf der Staat sie nicht vor sich selbst schützen.[91]

Durch eine Verhinderung der Preisgabe würde vielmehr das Ziel der Unterstützung der Persönlichkeitsentwicklung konterkariert: Die selbstbestimmte Preisgabe dient gerade der Persönlichkeitsentfaltung, welche durch staatliches Eingreifen verhindert würde. Somit ist kein grundgesetzliches Prinzip erkennbar, das den Schutz selbstbestimmt Preisgebender vor sich selbst gebieten würde. Jegliche Maßnahmen zur Verhinderung selbstbestimmter informationeller Preisgabe dienen damit keinem legitimen Zweck und sind somit nicht gerechtfertigt.

d) Rechtfertigung der Sicherung der Selbstbestimmung

Etwas anders gilt jedoch für Maßnahmen, die die Preisgabe nicht gänzlich verbieten, sondern die Selbstbestimmtheit der Preisgabe sichern, indem sie ihre Rahmenbedingungen regeln. Der Schutz vor sich selbst ist ein legitimer Eingriffszweck, wenn die Gewährleistung einer freien und selbstbestimmten Entscheidung oder Handlung der Grundrechtsträger beabsichtigt wird.[92] Den Staat trifft hier eine entsprechende Schutzpflicht, die er durch die Unterstützung informationellen Selbstschutzes sowie in Ausnahmefällen durch den Einsatz von Entscheidungsarchitekturen erfüllen kann.[93] Soweit lediglich informationeller Selbstschutz unterstützt wird, fehlt es bereits am Eingriff in die Nutzerrechte, eine Rechtfertigung ist entbehrlich.

Werden ausnahmsweise Entscheidungsarchitekturen angewandt, bedürfen diese der Rechtfertigung. Die Sicherung der Selbstbestimmung stellt einen legitimen Zweck dar und die genannten Maßnahmen sind geeignet, diesen Zweck zu erreichen. Sie müssen jedoch auch erforderlich sein. In den Fällen, in denen die Unterstützung informationellen Selbstschutzes keinen Erfolg verspricht, ist der Einsatz von Entscheidungsarchitekturen erforderlich. Die Maßnahmen müssen schließlich angemessen sein, dürfen die Preisgebenden also nicht unverhältnismäßig belasten. Da solche Regelungen die Preisgabe nicht verhindern, sondern lediglich die Entscheidung der Preisgebenden beeinflussen, werden sie regelmäßig[94] auch das Kriterium der Angemessenheit erfüllen.

Unzulässig ist hingegen erzwungener Schutz, solange er lediglich der Sicherung der Selbstbestimmtheit einer Entscheidung dienen soll und bei typisierender Betrachtung nicht von der fehlenden Selbstbestimmtheit auszugehen ist. Kritisch zu

[90] *Rogosch*, Die Einwilligung im Datenschutzrecht, 2013, 98.

[91] So auch: *Bull*, Zweifelsfragen um die informationelle Selbstbestimmung, NJW 2006, 1617, 1619 und *Trute*, Verfassungsrechtliche Grundlagen, in: Roßnagel (Hrsg.), Handbuch Datenschutzrecht, 2003, 156, 180, Rn. 48.

[92] *Wietfeld*, Selbstbestimmung und Selbstverantwortung, 2012, 84.

[93] Siehe oben Kapitel 5,A.V.3.

[94] Etwas anders gilt im Fall von Entscheidungsarchitekturen, die so intensiv wirken, dass sie erzwungenem Schutz gleichkommen.

sehen ist daher der Beschluss des Bundesverfassungsgerichts aus dem Jahr 1983 zu den jungen Transsexuellen. Nach diesem ist es mit der Verfassung vereinbar, gesunden Menschen vollständige Geschlechtsumwandlungen vor dem 25. Lebensjahr zu versagen – auch wenn die Regelung im konkreten Fall wegen Verstoßes gegen Art. 3 Abs. 1 GG nichtig war.[95] In allen übrigen Lebensbereichen wird spätestens mit Erreichen der Volljährigkeit vorausgesetzt, dass die Bürger die Fähigkeit besitzen, auch weitreichende und schwierige Entscheidungen selbst zu fällen. Dass hingegen vor Erreichen des 25. Geburtstages pauschal davon auszugehen sein soll, dass es Menschen an der erforderlichen Selbstbestimmung fehlt, um sich für eine vollständige Geschlechtsumwandlung zu entscheiden, erscheint fragwürdig.

Ebenso nicht vollständig überzeugend ist das Verbot der Lebendorganspende zwischen nicht verwandten Personen. Jedenfalls nicht ausreichend ist es, wenn das Bundesverfassungsgericht die Verfassungsmäßigkeit dieses Verbots ohne tiefer gehende Begründung bejaht unter Hinweis darauf, dass es ein legitimes Gemeinwohlanliegen sei, Menschen davor zu bewahren, sich selbst einen größeren persönlichen Schaden zuzufügen.[96]

Den Vorrang des Selbstschutzes[97] jedenfalls verkennt der Entwurf des Beschäftigtendatenschutzgesetzes.[98] Dieser reagiert auf Literaturstimmen, die von einem Kräfteungleichgewicht zwischen Arbeitgebern und Arbeitnehmern beziehungsweise Bewerbern ausgehen, das schon nach geltendem Recht eine Freiwilligkeit ausschließen kann.[99] Dementsprechend enthält § 32l BDSG-E die pauschale Bestimmung, dass die Erhebung, Verarbeitung und Nutzung von Beschäftigtendaten durch die Arbeitgeber aufgrund einer Einwilligung der Beschäftigten abweichend von dem datenschutzrechtlichen Verbotsprinzip (§ 4 Abs. 1 BDSG) nur zulässig ist, soweit dies in den Vorschriften über den Beschäftigtendatenschutz ausdrücklich vorgesehen ist. Damit soll den „Besonderheiten des Beschäftigungsverhältnisses und der Situation der Beschäftigten Rechnung getragen“ werden.[100] Diesen Grundsatz präzisiert der Gesetzesentwurf an zahlreichen Stellen. So ist nach § 32 Abs. 6 Satz 2

---

[95] BVerfGE 60, 123 (132); dazu ausführlich: *Wielpütz*, Über das Recht, ein anderer zu werden und zu sein, 2012, 52 ff.

[96] BVerfG NJW 1999, 3399, 3401; ablehnend auch: *Schroth*, Die Begrenzung des Spenderkreises im Transplantationsgesetz als Problem der paternalistischen Einschränkung menschlicher Freiheit, in: Schünemann/Müller/Philipps (Hrsg.), Das Menschenbild im weltweiten Wandel der Grundrechte, 2002, 35, 39 ff.

[97] Siehe zur Schutzbedürftigkeit als Voraussetzung für das Entstehen einer Schutzpflicht oben Kapitel 5,A.III.

[98] Entwurf eines Gesetzes zur Regelung des Beschäftigtendatenschutzes, BT-Drs. 17/4230 v. 15.12.2010. Auch der ursprüngliche Entwurf der EU-Datenschutz-Grundverordnung bestimmt in Art. 7 Abs. 4 EU-DS-GVO-E die Unwirksamkeit der Einwilligung im Falle eines erheblichen Ungleichgewichts zwischen den Positionen der Betroffenen und der für die Verarbeitung Verantwortlichen.

[99] *Rogosch*, Die Einwilligung im Datenschutzrecht, 2013, 92 ff. m. w. N.

[100] Begründung zum Entwurf eines Gesetzes zur Regelung des Beschäftigtendatenschutzes, BT-Drs. 17/4230 v. 15.12.2010, S. 22.

BDSG-E die Erhebung allgemein zugänglicher personenbezogener Daten aus sozialen Netzwerken ohne Mitwirkung der Beschäftigten auch dann nicht zulässig, wenn die Beschäftigten vorher auf die Erhebung hingewiesen wurden. Nach § 32a Abs. 1 Satz 4 BDSG-E darf den Arbeitgebern das vollständige Ergebnis einer ärztlichen Untersuchung der Arbeitnehmer trotz deren Einwilligung nicht mitgeteilt werden. Vergleichbares sieht § 32a Abs. 2 Satz 5 BDSG-E vor für das vollständige Ergebnis eines Eignungstests, wenn die durchführenden Personen einer Schweigepflicht unterlagen. In der Praxis bleibt abzuwarten, inwieweit diese strengen Grundsätze überhaupt Gesetzeskraft erlangen oder jedenfalls im Rahmen bestehender Arbeitsverhältnisse durch pauschale Einwilligungen im Rahmen von Betriebs- und Dienstvereinbarungen gelockert werden können. Diese gelten nach § 4 Abs. 1 BDSG-E als Rechtsvorschrift.

Auch angesichts des häufigen Kräfteungleichgewichts im Arbeitskontext erscheint es ungerechtfertigt, im Rahmen der Typisierung von einer so verbreiteten Übermacht der Arbeitgeber auszugehen, dass Bewerbern und Arbeitnehmern grundlegend das Recht zur informationellen Preisgabe gegenüber ihren Arbeitgebern abgesprochen werden dürfte.[101] Vielmehr muss eine Balance gefunden werden, die denjenigen Bewerbern und Arbeitnehmern, die sich selbstbestimmt für die Preisgabe von Daten entscheiden wollen, um damit beispielsweise Vorteile bei der Einstellung zu erhalten, dies ermöglicht. Dabei darf auch auf Typisierungen zurückgegriffen werden, diese müssen sich jedoch auf besonders kritische Bereiche beschränken.[102]

2. Rechtfertigung hinsichtlich der Rechte der verantwortlichen Stellen

Weiter könnten durch die Verhinderung informationeller Preisgabe die Rechte der verantwortlichen Stellen verletzt werden.

a) Evaluationsmaßstäbe zur Berufsfreiheit

Zunächst könnte in die Berufsfreiheit (Art. 12 Abs. 1 GG) der verantwortlichen Stellen eingegriffen werden. Im Rahmen eines einheitlichen Grundrechts gewährleistet Art. 12 Abs. 1 GG die freie Berufswahl und -ausübung.[103] Erfasst ist damit auch das Recht der verantwortlichen Stellen, ohne Verpflichtung zur Umsetzung von Schutzmaßnahmen ihr Geschäft auszuüben und als Grundlage ihres Geschäftsmodells jedenfalls mit Einwilligung der Betroffenen personenbezogene Daten erheben und verarbeiten zu können.

Fraglich ist, ob Maßnahmen zur Verhinderung informationeller Preisgabe einen Eingriff in die Berufsfreiheit darstellen.

---

[101] Wohl zustimmend: *Rogosch*, Die Einwilligung im Datenschutzrecht, 2013, 97.

[102] Denkbar wäre etwa ein typisierender Schutz für Bewerber und Arbeitnehmer, die (noch) keinen vollen Kündigungsschutz genießen.

[103] St. Rspr., seit: BVerfGE 7, 377 (400 ff.).

Ein erzwungener Schutz hat bereits nach dem klassischen Eingriffsbegriff Eingriffscharakter.

Die Unterstützung informationellen Selbstschutzes stellt einen Eingriff dar, wenn die verantwortlichen Stellen zur Umsetzung der Maßnahmen verpflichtet werden und es dadurch zu einer tatsächlichen Grundrechtsbeeinträchtigung kommt. Erforderlich ist dabei das Vorliegen einer berufsregelnden Tendenz des Eingriffs.[104] Ein Eingriff kann vorliegen, wenn verantwortliche Stellen gezwungen werden, ihr Angebot in einer bestimmten Weise zu gestalten, also beispielsweise Informationen anzubieten.[105] Geben Nutzer hingegen in der Folge der Unterstützung informationellen Selbstschutzes weniger Daten preis, geschieht dies aufgrund ihres autonomen Entschlusses. Die Unterstützungsmaßnahmen bezwecken keine Verhinderung der Preisgabe, sondern sollen lediglich eine selbstbestimmte Entscheidung der Nutzer ermöglichen. Dass unter Umständen weniger Daten preisgegeben werden, ist nicht notwendige Folge der Unterstützungsmaßnahme und dem Staat daher auch nach dem modernen Eingriffsbegriff nicht zurechenbar.

Entscheidungsarchitekturen kommt Eingriffscharakter zu, wenn die verantwortlichen Stellen zur Umsetzung der Maßnahmen verpflichtet werden und die Beeinträchtigung nicht nur marginal ist. Da Entscheidungsarchitekturen, anders als die Unterstützung informationellen Selbstschutzes, sehr häufig zum Unterbleiben der Preisgabe führen und dies überdies der staatlichen Intention entspricht, ist das durch Entscheidungsarchitekturen herbeigeführte Nichterhalten der Daten als Eingriff zu werten.

Die Berufsfreiheit der verantwortlichen Stellen kann nach dem – entgegen dem Wortlaut auch für die Berufswahl geltenden – Gesetzesvorbehalt des Art. 12 Abs. 1 Satz 2 GG eingeschränkt werden. Voraussetzung für die Rechtfertigung von Maßnahmen zur Verhinderung informationeller Preisgabe ist wiederum das Vorliegen eines formell und materiell verfassungsmäßigen Gesetzes, bei dessen Anwendung insbesondere der Verhältnismäßigkeitsgrundsatz zu wahren ist. Die Maßnahme muss also geeignet, erforderlich und angemessen zur Erreichung eines legitimen Zwecks sein. Gemäß der vom Bundesverfassungsgericht im Apothekerurteil entwickelten, in dieser Striktheit jedoch schon länger nicht mehr angewendeten, Drei-Stufen-Theorie ist hinsichtlich der Anforderungen an den Zweck danach zu differenzieren, ob eine Berufsausübungsregelung, eine subjektive Voraussetzung der Berufszulassung oder eine objektive Bedingung für die Berufszulassung vorliegt.[106] Auf der niedrigsten Stufe steht die reine Berufsausübungsregelung, die auf die Freiheit der Berufswahl nicht zurückwirkt, sondern nur bestimmt, in welcher Art und Weise die Berufstätigkeit zu gestalten ist.[107] Maßnahmen zur Verhinderung informationeller Preisgabe schreiben lediglich vor, wie die verantwortlichen Stellen ihre

[104] St. Rspr., BVerfGE 70, 191 (214).
[105] BVerfGE 95, 173 (181).
[106] St. Rspr., seit: BVerfGE 7, 377 (405 ff.).
[107] St. Rspr., seit: BVerfGE 7, 377 (405 f.).

Produkte anbieten können oder regeln die Art und Weise, in der sie die zur Berufsausübung benötigten personenbezogenen Daten erhalten. Die Berufszulassung wird nicht tangiert, es liegt vielmehr lediglich eine Regelung der Berufsausübung vor. Diese kann beschränkt werden, wenn vernünftige Erwägungen des Gemeinwohls dies zweckmäßig erscheinen lassen.[108]

Hinsichtlich der generellen Anforderungen an die übrige Verhältnismäßigkeitsprüfung (also des legitimen Zwecks und der Stufen der Verhältnismäßigkeitsprüfung) kann im Wesentlichen nach oben[109] verwiesen werden. Zu beachten ist dabei insbesondere, dass den verantwortlichen Stellen Handlungs- oder Unterlassungspflichten auferlegt werden können, wobei Unterlassungspflichten im Regelfall milder wirken als Handlungspflichten. Ebenso kann erwogen werden, die verantwortlichen Stellen ohne Eingriff zur Aufgabe des schädigenden Verhaltens zu bewegen, etwa durch wirtschaftliche Anreize.[110] Bei gleicher Effektivität kann ein solches Vorgehen zur Erfüllung des Verhältnismäßigkeitsgrundsatzes notwendig sein.[111] Schließlich sind Maßnahmen für die verantwortlichen Stellen gar nicht oder weniger eingriffsintensiv, wenn sie sich nicht gegen sie, sondern gegen die Nutzer richten (und vice versa). Die staatliche Vermittlung von Privatheitsbildung ist beispielsweise gegenüber den verantwortlichen Stellen ein milderes Mittel als Unterrichtungspflichten, die diesen auferlegt werden.

b) Evaluationsmaßstäbe zu anderen möglicherweise beeinträchtigten Rechten

Nicht einschlägig ist hingegen im Regelfall die Eigentumsgarantie gemäß Art. 14 Abs. 1 Satz 1 GG. Auch wenn Maßnahmen zur Umsetzung der Verhinderung informationeller Preisgabe den verantwortlichen Stellen Kosten auferlegen können, steht regelmäßig deren wirtschaftliches Erwerbsinteresse und nicht ihr Interesse am Erhalt ihres Eigentums im Vordergrund.

Ebenfalls von untergeordneter Bedeutung ist der Schutz durch die Meinungsfreiheit (Art. 5 Abs. 1 Satz 1, 1. Var. GG) davor, zur Verbreitung staatlicher Botschaften verpflichtet zu werden. Sowohl die Unterstützung informationellen Selbstschutzes als auch Entscheidungsarchitekturen könnten solche Botschaften enthalten. Die Meinungsfreiheit ist auf juristische Personen anwendbar (Art. 19 Abs. 3 GG)[112] und enthält auch die Komponente der negativen Meinungsfreiheit als Recht, eine Meinung nicht haben und äußern zu müssen.[113] In seinem Beschluss zur Tabakwerbung führt das Bundesverfassungsgericht jedoch zutreffend aus, dass die Verpflichtung zum Abdrucken von staatlichen Warnhinweisen Tabakhändler und -produzenten nicht hinsichtlich der Meinungsfreiheit, sondern nur hinsichtlich ihrer beruflichen

[108] St. Rspr., statt vieler: BVerfGE 7, 377 (405).
[109] Siehe oben Kapitel 6,A.I.1.a).
[110] *Krings*, Grund und Grenzen grundrechtlicher Schutzansprüche, 2003, 264.
[111] *Stern*, Das Staatsrecht der Bundesrepublik Deutschland III/1, 1988, § 67, V 2.
[112] Maunz/Dürig-GG/*Grabenwarter*, 2014, Art. 5, Rn. 32 ff.
[113] So das Obiter Dictum in: BVerfGE 65, 1 (40).

Außendarstellung tangiert.[114] Etwas anderes könnte lediglich gelten, wenn nicht deutlich erkennbar wäre, dass es sich um staatliche Warnhinweise handelt und die Konsumenten die Hinweise daher den Händler und Produzenten zurechnen könnten.[115] Unter Berücksichtigung dieser Rechtsprechung ist davon auszugehen, dass, wenn verantwortliche Stellen zur Umsetzung von Maßnahmen zur Verhinderung informationeller Preisgabe verpflichtet werden, nicht deren Meinungsfreiheit im Vordergrund steht, sondern ihr wirtschaftliches Interesse an der Vermeidung der Umsetzungskosten und eines Umsatzrückgangs. Anders als in den Vereinigten Staaten[116] ist daher nicht auf die Meinungsfreiheit als ausschlaggebendes Recht abzustellen.

Soweit ausnahmsweise weder Art. 12 Abs. 1 GG noch Art. 14 Abs. 1 Satz 1 GG noch Art. 5 Abs. 1 Satz 1, 1. Var. GG Schutz gewährleisten, ist die subsidiäre wirtschaftliche Betätigungsfreiheit der verantwortlichen Stellen einschlägig. Diese schützt als Auffanggrundrecht jedes Verhalten, das maßgeblich von Erwerbsmotiven geprägt ist oder typischerweise in objektiven Erwerbszusammenhängen erfolgt und nicht bereits anderweitig erfasst ist.[117]

Auch wenn mehrere Grundrechte der verantwortlichen Stellen durch die Maßnahmen zur Verhinderung der Preisgabe berührt werden könnten, ist regelmäßig nur die Berufsfreiheit nach Art. 12 Abs. 1 GG (in ihrer Ausprägung als Wettbewerbsfreiheit) einschlägig. Auf ihr soll im Weiteren der Fokus liegen.

c) Anwendung auf den konkreten Fall

Mit den Rechten der Preisgebenden vereinbar sind lediglich die Unterstützung informationellen Selbstschutzes und Maßnahmen der Entscheidungsarchitektur und das nur mit dem Ziel, die Selbstbestimmung zu schützen.[118] Fraglich ist, ob diese Maßnahmen auch mit der Berufsfreiheit der verantwortlichen Stellen in Einklang stehen.

Die Sicherung der Selbstbestimmung der Preisgebenden stellt einen legitimen Zweck dar. Beide Maßnahmenkategorien sind auch zur Erreichung dieses Zwecks geeignet. Regelmäßig wird lediglich die Unterstützung informationellen Selbstschutzes erforderlich sein, nur in Ausnahmefällen kann auf Entscheidungsarchitekturen zurückgegriffen werden. Soweit den verantwortlichen Stellen keine exorbitanten Umsetzungsmühen auferlegt werden, sind die Maßnahmen auch angemessen.

Zusammenfassend ist es mit den Rechten der Preisgebenden und der verantwortlichen Stellen vereinbar, zur Sicherung der Selbstbestimmung der Preisgebenden

---

[114] BVerfGE 95, 173 (181).
[115] BVerfGE 95, 173 (182).
[116] Siehe unten Kapitel 6,B.I.2.
[117] Maunz/Dürig-GG/*Di Fabio*, 2013, Art. 2, Rn. 81.
[118] Siehe oben Kapitel 6,A.I.1.d).

informationellen Selbstschutz zu unterstützen sowie, soweit erforderlich, Entscheidungsarchitekturen anzuwenden.

II. Rechtfertigung des Schutzes nicht selbstbestimmt Preisgebender

Weiter ist nach der Verfassungsmäßigkeit von erzwungenem Schutz der nicht selbstbestimmt Preisgebenden vor sich selbst zu fragen. Eine entsprechende Schutzpflicht besteht.[119] Diese gilt auch im Grenzbereich zwischen selbstbestimmter und nicht selbstbestimmter Preisgabe, wenn bei typisierender Betrachtung von der fehlenden Selbstbestimmtheit auszugehen ist. Der Eingriff dient dann dazu, die Selbstbestimmung der Preisgebenden herzustellen. Aus diesem Ziel ergibt sich bereits, dass ein Eingriff nur solange legitimiert sein kann, bis das Autonomiedefizit behoben wurde oder feststeht, dass keines bestand.[120]

Der erzwungene Schutz vor nicht selbstbestimmter Preisgabe müsste mit den Rechten der Preisgebenden (siehe I.1.a) und I.1.b)) sowie der verantwortlichen Stellen vereinbar sein (siehe I.2.a) und I.2.b)).

1. Rechtfertigung hinsichtlich der Rechte der Preisgebenden

Zweifelhaft ist, ob der Schutz der nicht selbstbestimmt Handelnden vor sich selbst überhaupt einen Eingriff in deren Grundrechte darstellt. Dies ließe sich bejahen mit dem Argument, staatliche Fremdbestimmung bleibe Fremdbestimmung, unabhängig von ihrem Ziel. Richtigerweise ist jedoch schon der Eingriff zu verneinen. Bei Fehlen der Fähigkeit zur Selbstbestimmung ist ein Eingriff in die Selbstbestimmung ausgeschlossen.[121] Wer nicht frei entscheiden kann, dem wird durch staatlichen Schutz auch keine Freiheit genommen.[122] Etwas anderes gilt nur, wenn durch die staatliche Schutzmaßnahmen in weitere Grundrechte eingegriffen wird, wie es beispielsweise im Rahmen der zwangsweisen Unterbringung psychisch Kranker der Fall ist. So stellt das Bundesverfassungsgericht in seiner Entscheidung zum Baden-Württembergischen Unterbringungsgesetz fest, dass auch die Unterbringung von nicht zurechnungsfähigen Personen nur unter Achtung des Verhältnismäßigkeitsgrundsatzes zulässig ist.[123] Da jedoch durch die Verhinderung informationeller Preisgabe nur eine Pseudo-Selbstbestimmung ausgeschlossen wird, ohne weitere Grundrechte zu beeinträchtigen, liegt kein Eingriff vor.[124]

---

[119] Die Unterstützung informationellen Selbstschutzes und Entscheidungsarchitekturen sind nicht geeignet zum Schutz der nicht selbstbestimmt Preisgebenden, sodass ihr (ausschließlicher) Einsatz eine Verletzung des Untermaßverbots darstellen würde: siehe oben Kapitel 5,A.VI.

[120] Vgl.: *Fateh-Moghadam*, Die Einwilligung in die Lebendorganspende, 2008, 29.

[121] *Mayr*, Grenzen des weichen Paternalismus II, in: Fateh-Moghadam/Sellmaier/Vossenkuhl (Hrsg.), Grenzen des Paternalismus, 2010, 48, 52.

[122] Vgl.: *Schwabe*, Der Schutz des Menschen vor sich selbst, JZ 1998, 66, 70.

[123] BVerfGE 58, 208, 226.

[124] Bejaht man hingegen das Vorliegen eines Eingriffs in die Rechte der nicht selbstbestimmt Preisgebenden, kann dieser gerechtfertigt werden. Das Bundesverfassungsgericht beurteilt in

2. Rechtfertigung hinsichtlich der Rechte der verantwortlichen Stellen

Der erzwungene Schutz bedarf der Rechtfertigung hinsichtlich des Eingriffs in die Rechte der verantwortlichen Stellen. Die auf gesetzlicher Grundlage angeordneten Maßnahmen müssen damit insbesondere verhältnismäßig sein.

Der erzwungene Schutz dient der Erfüllung der Schutzpflicht hinsichtlich des Rechts auf informationelle Selbstbestimmung und der Informationsfreiheit der nicht selbstbestimmt Preisgebenden. Die Erfüllung der Schutzpflicht stellt eine vernünftige Erwägung des Gemeinwohls dar, sodass ein legitimer Zweck vorliegt.[125] Da nicht selbstbestimmt Preisgebende gerade nicht zu selbstbestimmtem Handeln veranlasst werden können, ist lediglich erzwungener Schutz geeignet. Weiter muss er erforderlich sein. Da erzwungener Schutz generell und verbindlich wirkt, ist er regelmäßig effektiver als jedes andere weniger belastende Mittel. Mangels Existenz eines gleich wirksamen Mittels ist die Erforderlichkeit zu bejahen. Schließlich darf die Einschränkung der Rechte der verantwortlichen Stellen durch erzwungenen Schutz nicht außer Verhältnis stehen zum Zweck der Verhinderung nicht selbstbestimmter Preisgabe. Da es kein schützenswertes Interesse der verantwortlichen Stellen gibt, von der fehlenden Selbstbestimmung der Preisgebenden zu profitieren, ist erzwungener Schutz gerechtfertigt.

Mit den Rechten der Preisgebenden und der verantwortlichen Stellen ist es somit vereinbar, zur Verhinderung nicht selbstbestimmter Preisgabe erzwungenen Schutz anzuwenden. Dieser stellt das einzig wirksame Mittel dar.

III. Rechtfertigung des Schutzes von Allgemeinwohlbelangen

Schließlich könnte der Staat befugt sein, Maßnahmen zur Verhinderung informationeller Preisgabe zu treffen, wenn diese Allgemeinwohlbelange in Gestalt von Rechten Dritter oder allgemeiner gesellschaftlicher Belange gefährdet.[126] Während eine Pflicht zum Schutz der Rechte Dritter besteht, existiert keine Schutzpflicht hinsichtlich abstrakter gesellschaftlicher Belange.[127]

Zu klären ist, ob zur Verhinderung informationeller Preisgabe zum Schutz von Allgemeinwohlbelangen in die Rechte der Preisgebenden und in die der verantwortlichen Stellen eingegriffen werden darf.

---

ständiger Rechtsprechung Eingriffe in die persönliche Freiheit mit fürsorgerischem Charakter als verfassungsrechtlich zulässig: BVerfGE 10, 302 (324); 58, 208 (225). Da Eingriffe in die persönliche Freiheit regelmäßig schwerer wiegen als Eingriffe in das Recht auf informationelle Selbstbestimmung oder die Meinungs-, Informations- oder Berufsfreiheit, wären letztere a maiore ad minus ebenfalls rechtfertigbar.

[125] Zu den Anforderungen an den legitimen Zweck bei Berufsausübungsregelungen: BVerfGE 7, 377 (405).

[126] Zur Zuordnung von Rechten Dritter zu der Kategorie der Allgemeinwohlbelange: siehe oben Kapitel 3,A.III.

[127] Siehe oben Kapitel 5,A.VII.

1. Rechtfertigung hinsichtlich der Rechte der Preisgebenden

Es stellt sich die Frage, ob die Verhinderung von Gefahren für die bedrohten Allgemeinwohlbelange einen Eingriff in die Rechte der Preisgebenden rechtfertigen kann.

Voraussetzung ist zunächst das Vorliegen eines legitimen Zwecks. Sachgerecht erscheint es, danach zu unterscheiden, ob die Verhinderung von informationeller Preisgabe per se als verfassungsrechtlich geschützter Allgemeinwohlbelang gewertet werden kann oder ob es der Ableitung aus anderen Werten bedarf.

Denkbar wäre zunächst die Heranziehung eines öffentlichen Interesses am Bestand der Grundrechte. Es wird jedoch zutreffend darauf hingewiesen, dass wohl der Schutz jeder grundrechtlichen Position (vor Anderen und vor sich selbst) als im öffentlichen Interesse liegend subsumiert werden könnte.[128] Ein Ausufern der staatlichen Eingriffstatbestände wäre damit vorprogrammiert. Auch besteht zwar eine soziale Funktion der Grundrechte, diese darf sich jedoch nicht „auf Kosten ihrer individuellen Bedeutung auswirken“, da eine einseitige Akzentuierung der sozialen Funktion der Grundrechte die Individuen zu „Funktionären“ oder „Destinären“ degradieren könnte.[129]

Die Grundrechte entfalten objektiv-rechtliche Wirkung und haben als verfassungsrechtliche Grundentscheidung für alle Bereiche des Rechts Geltung.[130] Die objektive Grundrechtsfunktion dient jedoch, wie das Bundesverfassungsgericht im Mitbestimmungsurteil feststellt, der prinzipiellen Verstärkung der grundrechtlichen Geltungskraft und lässt sich nicht zu einem Gefüge objektiver Normen verselbstständigen, in dem der ursprüngliche und bleibende Sinn der Grundrechte zurücktritt.[131] Das Grundgesetz schützt auch die Freiheit zur Selbstschädigung und -gefährdung. Zwar plädieren Manche dafür, zum Schutz der „gesamte[n] Kommunikationsverfassung der Gesellschaft“ der Zustimmungsfähigkeit zu Datenerhebungen im Allgemeininteresse Grenzen zu setzen.[132] Diese Aussage wird jedoch richtigerweise sogleich relativiert, wenn ausschließlich Beispiele gravierend gefährdeter Selbstbestimmung genannt werden, ohne jedoch auf die hier gegenständlichen Konsequenzen selbstbestimmter, aber dennoch gesellschaftlich nachteiliger Preisgabe abzustellen. Nicht ausreichend ist entsprechend ein bloßes Interesse am gesamtgesellschaftlichen Erhalt von Privatheit.

Vielmehr bedarf es der Rückführung auf benennbare Gefahren, die aus der informationellen Preisgabe erwachsen können. Im Einklang mit dem Gedanken, dass Externalitäten nicht Unbeteiligten oder der Gesellschaft aufgebürdet werden dür-

---

[128] *Pietzcker*, Die Rechtsfigur des Grundrechtsverzichts, 17 Der Staat (1978), 527, 539 f.; skeptisch: *Hillgruber*, Der Schutz des Menschen vor sich selbst, 1992, 126 ff.

[129] *Häberle*, Die Wesensgehaltgarantie des Artikel 19 Abs. 2 Grundgesetz, ³1983, 10 f.

[130] Siehe oben Kapitel 5,A.I.

[131] BVerfGE 50, 290 (337).

[132] *Roßnagel/Pfitzmann/Garstka*, Modernisierung des Datenschutzrechts, DuD 2001, 253, 259.

fen,[133] kann ein Recht zu staatlichem Einschreiten bestehen, wenn das gefährdende Verhalten Interessen der Gesellschaft bedroht.[134] Informationelle Preisgabe kann direkte Auswirkungen auf die informationelle Privatheit Dritter sowie den gesellschaftlichen Fortschritt und die Demokratie haben. Die bedrohten Interessen genießen verfassungsrechtlichen Stellenwert.[135] Ihr Schutz kann damit einen Allgemeinwohlbelang darstellen, der eine Einschränkung der Rechte der Preisgebenden rechtfertigen kann.

Weiter müsste die staatliche Maßnahme geeignet zur Erreichung dieses Zwecks sein. Bei allen drei Maßnahmenkategorien – dem erzwungenen Schutz, der Unterstützung informationellen Selbstschutzes und den Entscheidungsarchitekturen – besteht jedenfalls die „abstrakte Möglichkeit der Zweckerreichung“,[136] sodass sie nach herrschender Ansicht geeignet sind. Jedoch ist zu bedenken, dass die Unterstützung informationellen Selbstschutzes häufig primär auf den Schutz der Individuen zielen und gerade keinen Schutz Dritter oder der Gesellschaft anstreben wird. Der Zweck kann daher, wenn überhaupt, nur mittelbar dadurch erreicht werden, dass gesamtgesellschaftlich weniger Daten preisgegeben werden. Soweit die Nutzer ihre informationelle Privatheit preisgeben möchten, bleiben diese Maßnahmen wirkungslos.[137] Fordert man für die Geeignetheit mit der vorzugswürdigen Ansicht einen nachvollziehbaren Wirkungszusammenhang zwischen Zweck und Mittel,[138] so fehlt es häufig an der Geeignetheit der Unterstützung informationellen Selbstschutzes. Entscheidungsarchitekturen hingegen können de facto zum Unterbleiben der Preisgabe führen und so den Zweck jedenfalls fördern. Erzwungener Schutz verhindert die Preisgabe und ist damit jedenfalls geeignet.

Weiter muss die Maßnahme erforderlich sein. Alle drei Maßnahmen sind in ihrer Wirkungsstufe jeweils das mildeste gleich wirksame Mittel und somit erforderlich.

Schließlich müssen die Maßnahmen angemessen sein, dürfen also die Rechte der Preisgebenden nicht unverhältnismäßig belasten.

Zwischen den Rechten Dritter und den Rechten der Preisgebenden ist ein Ausgleich im Wege der praktischen Konkordanz zu schaffen. Ergibt die individuelle Abwägung der kollidierenden Rechte ein Übergewicht der Rechtsgüter Dritter, ist der Eingriff in die Rechte der Preisgebenden gerechtfertigt.[139] Die erzwungene Verhinderung informationeller Preisgabe stellt das wirksamste Mittel dar und kann, wenn den Rechten der Dritten in der Abwägung ein größes Gewicht als den Rechten

[133] Siehe auch unten Kapitel 7,A.II.
[134] BVerfGE 22, 180 (219) und 30, 47 (53).
[135] Siehe oben Kapitel 3,B.II.2 und Kapitel 3,B.II.3.
[136] BVerfGE 100, 313 (373).
[137] *Solove* erkennt mit dieser Begründung strukturelle Probleme des „privacy self-managements“: *Solove*, Privacy Self-Management and the Consent Dilemma, 126 Harvard L. Rev. (2013), 1880, 1881, 1892 f.
[138] BVerfGE 107, 186 (197).
[139] In diesen Fällen wird regelmäßig eine entsprechende Schutzpflicht bestehen, deren Erfüllung die in Rede stehende Maßnahme ist: siehe oben Kapitel 5,A.VII.

der Preisgebenden zukommt, gerechtfertigt werden. Je nach Einzelfall können Entscheidungsarchitekturen vorzuziehen sein, da sie zwar weniger wirksam, aber auch weniger eingriffsintensiv sind. Da die Unterstützung informationellen Selbstschutzes leer läuft, sobald die Nutzer die Daten preisgeben möchten, ist sie regelmäßig nicht wirksam genug, um die informationelle Privatheit Dritter zu schützen.

Soweit keine Rechte Dritter, sondern lediglich abstrakte gesellschaftliche Belange betroffen sind, fällt die Abwägung anders aus. Bei dem gesellschaftlichen Fortschritt und der Demokratie handelt es sich um abstrakte Werte, die im Regelfall keine konkreten Individualinteressen berühren. Der verfassungsrechtliche Stellenwert gesellschaftlichen Fortschritts und der Demokratie ist zwar bei der Untersuchung staatlicher Möglichkeiten zur Verhinderung informationeller Preisgabe zu beachten. Allerdings sind die gesellschaftlichen Belange abstrakter Natur, eine Mitwirkungspflicht der Einzelnen, einen Beitrag zu gesellschaftlichem Fortschritt zu leisten, besteht nicht. Zudem besteht auch keine Pflicht der Einzelnen, die Kommunikationsgrundrechte in einer Weise zu nutzen, die der Demokratie förderlich wäre.[140] Einige Voraussetzungen für das Gedeihen der Demokratie schreibt das Grundgesetz als verpflichtend vor (Erziehungspflicht: Art. 6 Abs. 2 GG, Schulpflicht: Art. 7 GG, Möglichkeit zur Einführung einer Wehrpflicht: Art. 12a GG). Daraus, dass das Grundgesetz bei der für die Demokratie essenziellen Beteiligung der Bürger durch Wahlen in Art. 38 GG ein Wahlrecht, keine -pflicht („Wahlberechtigt“) konstituiert, muss geschlossen werden, dass das Grundgesetz gerade nicht von einer Pflicht zur Partizipation im demokratischen Prozess ausgeht.[141]

Sollen der Schutz gesellschaftlicher Belange oder der Demokratie aber Grundlage dafür sein, informationelle Preisgabe zu verhindern und damit in die Rechte von Individuen einzugreifen, bedarf es einer sorgfältigen Abwägung. Insofern muss im Rahmen der Verhältnismäßigkeitsprüfung ein strenger Maßstab angelegt werden, um nicht de facto entsprechende Mitwirkungspflichten einzuführen. Da das Grundgesetz gerade keine Pflicht zur Mitwirkung an gesellschaftlichem Fortschritt oder an der Demokratie kennt, sind den Preisgebenden nur die schonenderen Maßnahmen zuzumuten, mithin also die Entscheidungsarchitekturen und die Unterstützung informationellen Selbstschutzes. Erzwungener Schutz zum Zwecke der Wahrung von gesellschaftlichem Fortschritt sowie der Demokratie ist derzeit wohl unzumutbar und nicht gerechtfertigt. Auch hinsichtlich der Entscheidungsarchitekturen ist Zurückhaltung geboten. Diese zwingen die Nutzer zwar nicht zu bestimmtem Verhalten, führen jedoch de facto häufig eine Verhaltensänderung herbei und stellen somit einen massiven Eingriff dar. Eine Rechtfertigung dieser Maßnahmen zum Schutz vor Gefahren, die informationelle Preisgabe für die Gesellschaft birgt, ist

140 In diese Richtung argumentiert auch: *Starck*, Grundrechtliche und demokratische Freiheitsidee, in: Isensee/Kirchhof (Hrsg.), Handbuch des Staatsrechts der Bundesrepublik Deutschland III, 2005, 3 ff. Rn. 39.

141 Zu diesem Ergebnis kommt auch: *Littwin*, Grundrechtsschutz gegen sich selbst, 1993, 177 f.

daher nur in Ausnahmefällen möglich. Mangels eines Eingriffs in die Nutzerrechte[142] bleibt die Unterstützung informationellen Selbstschutzes immer möglich, auch wenn sie nur bedingt wirksam ist.

Etwas anderes kann jedoch in Zukunft gelten, wenn konkrete, greifbare und weitreichende Gefahren für das Allgemeinwohl absehbar werden. So wäre auch erzwungener Schutz beispielsweise gerechtfertigt, wenn Bürger ihre Entscheidungen im Rahmen politischer Wahlen nicht mehr selbst treffen würden, sondern unabänderlich durch einen Computer mangels Analyse ihrer personenbezogenen Daten erstellen lassen würden.

2. Rechtfertigung hinsichtlich der Rechte der verantwortlichen Stellen

Weiter können alle drei Maßnahmen einen Eingriff in die Rechte der verantwortlichen Stellen darstellen,[143] dessen verfassungsrechtliche Rechtfertigung zu prüfen ist. Hinsichtlich der Geeignetheit und Erforderlichkeit ergeben sich keine Änderungen zu 1, sodass lediglich die Angemessenheit infrage steht.

Ein schützenswertes Interesse der verantwortlichen Stellen an einer Preisgabe, die die Rechte Dritter verletzt, besteht nicht. Daher können alle drei Maßnahmen gerechtfertigt werden, wobei erzwungener Schutz häufig das einzige wirksame Mittel ist.

Wird der Schutz abstrakter Allgemeinwohlbelange bezweckt, lassen sich schon hinsichtlich der Nutzerrechte nur der Einsatz der Unterstützung informationellen Selbstschutzes sowie von Entscheidungsarchitekturen rechtfertigen.[144] Auch in Bezug auf die Rechte der verantwortlichen Stellen ist daher nur die Angemessenheit dieser beiden Maßnahmekategorien zu prüfen. Da verantwortliche Stellen, also im Regelfall Unternehmen, verfassungsrechtlich nicht direkt zur Mitwirkung am gesellschaftlichen Fortschritt und der Demokratie verpflichtet sind, sind ihnen keine schwerwiegenden Eingriffe zuzumuten. Findet überhaupt ein Eingriff in ihre Rechte statt, muss sich dieser im geringstmöglichen Rahmen halten.

Die Unterstützung informationellen Selbstschutzes stellt nicht in jedem Fall einen Eingriff dar, sondern nur, wenn die verantwortlichen Stellen zur Umsetzung verpflichtet werden und ihnen dadurch erhebliche Beeinträchtigungen entstehen. Vor diesem Hintergrund muss der Schwerpunkt auf solcher Unterstützung informationellen Selbstschutzes liegen, die ohne eine verpflichtende Umsetzung durch die verantwortlichen Stellen auskommt. Als Beispiel genannt werden kann Datenschutz als Bildungsauftrag.[145] Alternativ können die verantwortlichen Stellen durch Anrei-

[142] Siehe oben Kapitel 6,A.I.1.a).
[143] Zum Eingriffscharakter von erzwungenem Schutz, der Unterstützung informationellen Selbstschutzes und Entscheidungsarchitektur: siehe oben Kapitel 6,A.I.2.a).
[144] Siehe oben Kapitel 6,A.III.1.
[145] Siehe oben Kapitel 4,B.IV.

ze (etwa steuerliche Vergünstigungen oder Vorrang bei der Vergabe öffentlicher Aufträge) zur Implementierung von Entscheidungsarchitekturen bewegt werden.

Soweit dies nicht möglich ist, können die verantwortlichen Stellen zur Umsetzung von Maßnahmen zur Unterstützung informationellen Selbstschutzes verpflichtet werden. Nur in Ausnahmefällen ist schließlich der verpflichtende Einsatz von Entscheidungsarchitekturen zulässig.

B. Rechtfertigung nach US-Verfassungsrecht

Das US-Recht kennt, anders als das deutsche, keine verfassungsrechtliche Pflicht zur Verhinderung informationeller Preisgabe.[146] Zu prüfen ist, inwieweit staatliche Schritte zur Verhinderung informationeller Preisgabe in den Vereinigten Staaten verfassungsrechtlich gerechtfertigt werden können.

Im Folgenden werden die Rechtfertigungsmöglichkeiten von Maßnahmen zum Schutz der selbstbestimmt Preisgebenden (siehe I), der nicht selbstbestimmt Preisgebenden (siehe II) und des Allgemeinwohls analysiert (siehe III).

I. Rechtfertigung des Schutzes selbstbestimmt Preisgebender

Zunächst ist zu untersuchen, ob eine staatliche Befugnis zum Schutz selbstbestimmt Preisgebender besteht.

1. Rechtfertigung hinsichtlich der Rechte der Preisgebenden

Durch Maßnahmen zum Schutz selbstbestimmt Preisgebender vor sich selbst könnte in deren Rechte eingegriffen werden. Die Unterstützung informationellen Selbstschutzes stellt auch im US-Recht keinen Eingriff in die Rechte der Preisgebenden dar, da ihnen lediglich zusätzliche Optionen geboten werden, ohne sie jedoch an der Ausübung ihrer Rechte zu hindern.

Zu prüfen ist daher nur, ob staatliche Maßnahmen zur Verhinderung informationeller Preisgabe durch erzwungenen Schutz oder Entscheidungsarchitekturen in die Rechte der Preisgebenden eingreifen und ob diese Eingriffe gerechtfertigt werden können.

a) Evaluationsmaßstäbe zur Redefreiheit

Die Maßnahmen könnten in die Redefreiheit der Preisgebenden eingreifen. Informationelle Preisgabe kann explizit (also bewusst und zielgerichtet) sowie implizit (also technisch im Hintergrund und regelmäßig unbewusst) erfolgen (siehe Kapitel 2,B). Es sind drei Konstellationen zu unterscheiden: die Verhinderung expliziter Preisgabe durch erzwungenen Schutz (siehe aa)), die Verhinderung expliziter Preis-

---

[146] Siehe oben Kapitel 5,B.

gabe durch Entscheidungsarchitekturen (siehe bb)) sowie die Verhinderung impliziter Preisgabe (siehe cc)).

aa) Verhinderung expliziter Preisgabe durch erzwungenen Schutz

Das Recht der Nutzer zur expliziten informationellen Preisgabe wird durch die Redefreiheit nach dem Ersten Zusatzartikel[147] geschützt. Nach diesem darf der Kongress[148] kein Gesetz erlassen, das die Redefreiheit verkürzen würde. Geschützt sind sowohl der Akt des Sprechens als auch der des Zuhörens. Auch das Veröffentlichen von Inhalten im Internet durch Individuen ist eingeschlossen.[149] Nicht erfasst ist ein Recht zum Besitz, Konsum, Vertrieb oder der Herstellen obszönen Materials,[150] es sei denn, dies geschieht in den eigenen vier Wänden.[151] Informationelle Preisgabe, die sich auf obszönes Material erstreckt, erfährt daher von vornherein keinen Schutz und kann verboten werden.

Abhängig von der Art des Eingriffs in die Redefreiheit finden verschiedene Rechtfertigungsanforderungen Anwendung:

Gemäßigte Rechtfertigungsanforderungen (die sogenannte Intermediate Scrutiny) gelten, wenn nur Zeit, Ort und Modalitäten der Rede reguliert werden sollen. Die Rede kann dann eingeschränkt werden, wenn die Maßnahme einen wichtigen oder substanziellen staatlichen Zweck fördert und die Einschränkung der Redefreiheit nicht stärker als notwendig ist, um den Zweck zu erreichen.[152] Soweit den Einzelnen jedoch beispielsweise eine bestimmte Rede mittels einer Vielzahl von Internettechnologien unter dem Hinweis verboten wird, es stünde ihnen frei, eine eigene Webseite mit entsprechenden Sicherheitseinstellungen einzurichten, handelt es sich um eine gegen den Inhalt der Meinungsäußerung gerichtete Maßnahme.[153] Erst recht kann ein Verbot der informationellen Preisgabe im Internet trotz der Möglichkeit, Daten offline preiszugeben, nicht als bloße Regelung der Modalitäten gewertet

---

[147] Zur ebenfalls durch den Ersten Zusatzartikel geschützten Informationsfreiheit: siehe oben Kapitel 3,C.I.4.

[148] Der Erste Zusatzartikel findet über den 14. Zusatzartikel Anwendung auf das Handeln der Bundesstaaten: Gitlow v. People of State of New York, 268 U.S. 652, 666 (1925).

[149] Reno v. American Civil Liberties Union, 521 U.S. 844, 853 (1997).

[150] Der U.S. Supreme Court führt aus: „All ideas having even the slightest redeeming social importance – unorthodox ideas, controversial ideas, even ideas hateful to the prevailing climate of opinion – have the full protection of the guaranties, unless excludable because they encroach upon the limited area of more important interests. But implicit in the history of the First Amendment is the rejection of obscenity as utterly without redeeming social importance. This rejection for that reason is mirrored in the universal judgment that obscenity should be restrained, reflected in the international agreement of over 50 nations, in the obscenity laws of all of the 48 States, and in the 20 obscenity laws enacted by the Congress from 1842 to 1956.“: Roth v. United States, 354 U.S. 476, 484 f. (1957) m. w. N.

[151] Stanley v. Georgia, 394 U.S. 557, 565 (1969).

[152] United States v. O'Brien, 391 U.S. 367, 376 f. (1968).

[153] Reno v. American Civil Liberties Union, 521 U.S. 844, 879 f. (1997).

werden. Zur Rechtfertigung der Verhinderung informationeller Preisgabe ist die Intermediate Scrutiny daher nicht ausreichend.

Wenn sich die Maßnahme gegen den Inhalt der Meinungsäußerung richtet, also Rede verhindert wird, werden strenge Rechtfertigungsanforderungen (die sogenannte Strict Scrutiny) angewandt.[154] Dies ist beispielsweise der Fall, wenn zum Schutz Minderjähriger Inhalte im Internet nicht veröffentlicht werden dürfen.[155] Zur Rechtfertigung muss dann ein zwingender staatlicher Zweck (Compelling State Interest) verfolgt werden, der nicht auch durch weniger restriktive Mittel gleich wirksam erreicht werden kann.[156] Die Verhinderung der Preisgabe personenbezogener Daten kann nur nach der Strict Scrutiny gerechtfertigt werden, wie sich beispielsweise an der nicht rechtskräftig gewordenen Entscheidung des District Court im Zentralen Distrikt von Kalifornien[157] zum „Don't ask, don't tell"-Gesetz im US-Militär[158] zeigt. Nach diesem Gesetz war es Homosexuellen zwar gestattet, im US-Militär zu dienen, jedoch nur, solange sie ihre sexuelle Ausrichtung nicht preisgaben. Gleichzeitig durfte der Staat nicht nach der sexuellen Ausrichtung fragen. Dadurch wurde gegen die Redefreiheit der Betroffenen verstoßen.

Wird explizite informationelle Preisgabe durch erzwungenen Schutz verhindert, wird damit bestimmte Rede wegen ihres Inhalts unterbunden. Es liegt damit ein Eingriff in die Rechte aus dem Ersten Zusatzartikel vor, zu dessen Rechtfertigung die Strict Scrutiny angewandt werden muss.

bb) Verhinderung expliziter Preisgabe durch Entscheidungsarchitekturen

Angesichts dessen, dass Entscheidungsarchitekturen die Preisgebenden einer staatlichen Botschaft aussetzen und sie damit zwingen, staatliche Rede zur Kenntnis zu nehmen, erscheint es denkbar, auch diese am Ersten Zusatzartikel zu messen. Diese Ansicht wird jedoch von den Gerichten nicht geteilt. In Texas Medical Providers Performing Abortion Services v. Lakey war der Fünfte Circuit Court mit einem Gesetz befasst, das schwangere Frauen vor einer Abtreibung dazu zwang, ihr Kind per Ultraschall zu betrachten, das Herzklopfen des Kindes zu hören, sich die medi-

---

[154] Dies ist immer dann der Fall, wenn nicht nur die Modalitäten der Rede eingeschränkt werden, sondern die Rede verhindert. Nicht erforderlich ist, dass die Rede gezielt aufgrund eines bestimmten Inhalts verhindert wird. Zum Vergleich: In Deutschland darf eine Meinungsäußerung nicht durch Sonderrecht eingeschränkt werden, sondern nur durch allgemeine Gesetze, siehe: BVerfGE 7, 198 (209); 111, 147 (155) und oben Kapitel 6,A.I.1.b).

[155] Reno v. American Civil Liberties Union, 521 U.S. 844, 874 (1997).

[156] Die Idee der Strict Scrutiny geht zurück auf: United States v. Carolene Products Co., 304 U.S. 144, 152, Fn. 4 (1938).

[157] Log Cabin Republicans v. United States, 716 F.Supp.2d 884 (C.D. Cal. 2010) (nicht rechtskräftig). Da das Gesetz in der Reaktion auf die Entscheidung abgeschafft wurde, erübrigte sich eine letztinstanzliche Entscheidung: Log Cabin Republicans v. United States, 658 F.3d 1162 (9th Cir. 2011).

[158] 10 U.S.C. § 654 a. F. Dieses Prinzip konnte als einfachgesetzlich auferlegte Pflicht zur Wahrung der Privatheit bezeichnet werden: *Cohen*, Regulating Intimacy, 2002, 78 ff.

zinischen Erkenntnisse, die sich aus beiden Untersuchungen ergaben, im Detail erklären zu lassen und im Anschluss an diese Prozedur 24 Stunden vor Durchführung der Abtreibung zu warten. Das Argument, den Frauen würde damit staatliche Rede aufgezwungen, lehnt das Gericht ab.[159] Wird durch diese Maßnahme die Entscheidung der Frauen beeinflusst, geht dies nicht auf eine ideologische staatliche Maßnahme zurück, sondern auf eine Kombination ihrer neu gewonnenen Erkenntnisse und ihrer persönlichen Werte.[160]

In der Entscheidung des D.C. Circuit Court zu Grafiken auf Zigarettenschachteln finden die gemäß dem Ersten Zusatzartikel garantierten Rechte der Rauchenden gar keine Erwähnung, obwohl die Käufer dem Anblick der Grafiken und somit den staatlichen Botschaften ausgesetzt sind.[161]

Vereinzelt wird gefordert, für Maßnahmen, die Überzeugung und Verhalten der Betroffenen auf emotionale Weise beeinflussen sollen, einen Schutz durch den Ersten Zusatzartikel anzuerkennen.[162] Dies soll jedoch nur in den seltenen Fällen gelten, in denen die Betroffenen keine Möglichkeit zum Opt-out haben. Eine Auseinandersetzung mit dem libertär paternalistischen Argument, Entscheidungsarchitekturen dienten gerade dem individuellen Wohl, unterbleibt vollständig.

Die diskutierten Möglichkeiten der Entscheidungsarchitekturen[163] lassen den Einzelnen die Möglichkeit, die staatliche Botschaft zu ignorieren, sodass sie jedenfalls keinen Eingriff in den Ersten Zusatzartikel darstellen.

cc) Verhinderung impliziter Preisgabe

Schließlich ist zu klären, ob auch implizite Preisgabe geschützt ist. Über den Wortlaut hinaus ist die „expression of an idea through activity“ vom Ersten Zusatzartikel erfasst, wenn eine Absicht vorlag, eine bestimmte Nachricht zu übermitteln und es unter den gegebenen Bedingungen wahrscheinlich war, dass die Nachricht von den Zuschauern verstanden würde. Im Ausgangsfall hatte ein Student eine US-Flagge mit einem Peace-Symbol versehen und während des Vietnam-Krieges aufgehängt, was eine geschützte Meinungsäußerung darstellte.[164] Bloße implizite Preisgabe durch Aktivitäten, auf deren Grundlage Daten gesammelt werden können, ist allerdings nicht auf die Übermittlung einer Nachricht gerichtet, sodass nicht von einem Schutz durch den Ersten Zusatzartikel auszugehen ist.

---

159 „[S]uch laws are part of the state's reasonable regulation of medical practice and do not fall under the rubric of compelling 'ideological' speech that triggers First Amendment strict scrutiny“: Texas Medical Providers Performing Abortion Services v. Lakey, 667 F.3d 570, 576 (5th Cir. 2012).

160 „If the sonogram changes a woman's mind about whether to have an abortion […] that is a function of the combination of her new knowledge and her own 'ideology' […], not of any 'ideology' inherent in the information she has learned about the fetus.“ : Texas Medical Providers Performing Abortion Services v. Lakey, 667 F.3d 570, 577, Fn. 4 (5th Cir. 2012).

161 R.J. Reynolds Tobacco Co. v. Food and Drug Admin., 696 F.3d 1205 (D.C. Cir. 2012).

162 *Ferony*, Constitutional Law, 35 Western New England L. Rev. (2013), 205, 225 ff.

163 Siehe oben Kapitel 4,C.

164 Spence v. State of Wash, 418 U.S. 405, 410 f. (1974).

Ebenso liegt, wie auch in Deutschland,[165] kein Eingriff darin, dass Nutzer als Konsequenz der Verhinderung informationeller Preisgabe nicht mit personalisierten Angeboten versorgt werden. Ihr Zugang zu solchen Informationen wird nicht gehindert, sondern vielmehr eine unbeeinflusste Versorgung mit Quellen gefördert.

b) Evaluationsmaßstäbe zum prozessualen Due-Process-Schutz

Zu klären bleibt folglich, welche Anforderungen zu stellen sind an die Verhinderung expliziter Preisgabe durch Entscheidungsarchitekturen sowie an die Verhinderung impliziter Preisgabe durch erzwungenen Schutz und Entscheidungsarchitekturen.

Im Falle expliziter Preisgabe entscheiden sich Nutzer bewusst für diese. Implizite Preisgabe im Zusammenhang mit der Nutzung von Angeboten, die Daten erheben, wird jedenfalls von dem Willen der Nutzer getragen, die datenerhebenden Angebote zu nutzen. Dadurch können die Preisgebenden das wirtschaftliche Potenzial ihrer Daten ausnutzen. Solche Entscheidung zur Preisgabe werden durch die informationelle Privatheit geschützt.

Einzelne Aspekte der informationellen Privatheit haben Anerkennung als Fundamental Right gefunden und können damit nur nach Strict Scrutiny eingeschränkt werden.[166] Nicht anerkannt sind jedoch ein Recht, nicht durch Entscheidungsarchitekturen an expliziter Preisgabe gehindert zu werden sowie ein Recht, nicht von impliziter Preisgabe abgehalten zu werden.

Solche Maßnahmen genießen lediglich prozessualen Due-Process-Schutz und sind daher am Rational-Basis-Test zu messen, müssen also lediglich in einem nachvollziehbaren Verhältnis zu einem legitimen Zweck stehen.[167] Die Beweislast dafür, dass dies nicht der Fall ist, liegt bei demjenigen, der die Verletzung des prozessualen Due Process behauptet.[168]

c) Schutz vor sich selbst als legitimer Eingriffszweck

Die gewonnenen Erkenntnisse sind nun auf die Frage anzuwenden, ob die Verhinderung selbstbestimmter Preisgabe zum Schutz der Nutzer mit deren Rechten vereinbar ist. Die verschiedenen Konstellationen lassen sich wie folgt zusammenfassen:

Wird explizite Preisgabe durch erzwungenen Schutz verhindert, ist dies nur nach dem hohen Maßstab der Strict Scrutiny zulässig, es muss also ein zwingender staatlicher Zweck verfolgt werden, der nicht auch durch weniger restriktive Mittel gleich wirksam erreicht werden kann.

Alle anderen Fälle der Verhinderung informationeller Preisgabe sind nicht am Ersten Zusatzartikel zu messen, sondern genießen nur prozessualen Due-Process-

[165] Siehe oben Kapitel 6,A.I.1.b).
[166] Siehe oben Kapitel 3,C.I.3.a).
[167] Siehe oben Kapitel 3,C.I.3.b).
[168] United States v. Carolene Products Co., 304 U.S. 144, 152 (1938).

Schutz. Sie können daher nach dem Rational-Basis-Test gerechtfertigt werden, müssen also in einem nachvollziehbaren Verhältnis zu einem legitimen Zweck stehen.

Wieder stellt sich die Frage, ob der Schutz vor sich selbst einen legitimen Eingriffszweck darstellt: „Many of us allocate time and money and other resources in ways susceptible to just criticism by many standards. Nonetheless, our political ideals emphasize that the right to freely decide is of much greater significance than the quality of those choices actually made. It is never easy for one who is concerned and feels himself particularly knowledgable [sic] to observe others exercise their freedom in ways that to him appear unenlightened. As a nation, however, historically and continuously, we are irrevocably committed to the principle that the individual must be given maximum latitude in determining his own personal destiny.“[169]

Diese Zeilen bringen die überragende Stellung der freien Entscheidung der Individuen im US-Rechts- und Gesellschaftsverständnis zum Ausdruck. US-amerikanisches Recht ist geprägt von dem liberalen Grundgedanken der individuellen Freiheit, unabhängig davon, ob die Einzelnen diese Freiheit weise nutzen und mit der Konsequenz, dass sie die Folgen ihrer Fehlentscheidungen tragen als Preis für die Freiheit, ihre eigenen Fehler zu machen.[170]

Das Rechtssystem zeichnet sich aus durch Freiheitsliebe, moralische Vielfalt, Toleranz, staatliche Neutralität und begrenztes staatliches Einschreiten.[171] Hinzu tritt ein ausgeprägtes Vertrauen in die Marktwirtschaft. Ein Schutz der selbstbestimmt Preisgebenden vor sich selbst liefe dem diametral entgegen. Wenn überhaupt der Versuch gewagt werden soll, entgegen der Verfassungstradition selbstbestimmt Handelnde vor sich selbst zu schützen, müsste jedenfalls der Schutz eines ausgesprochen wichtigen Interesses bezweckt werden.

Durch informationelle Preisgabe können zum einen langfristig die informationelle Privatheit der Preisgebenden gefährdet werden sowie zum anderen Interessen, die durch ihre Informationsfreiheit geschützt werden.

Das US-Verfassungsrecht misst der informationellen Privatheit derjenigen, die diese selbst preisgeben, einen sehr geringen Stellenwert zu.[172] Schutz durch den Vierten Zusatzartikel besteht regelmäßig sogar aus mehreren Gründen nicht. Schlagkräftigstes Hindernis für einen Schutz ist die Third-Party-Doktrin, nach der der Schutz entfällt, sobald die Preisgebenden ihre Daten irgendwem (beispielsweise einem Internetanbieter) anvertraut haben. Auch das Right to Privacy gewährt keinen Schutz gegen Risiken, die dadurch entstehen, dass die Preisgebenden ihre Daten Privaten offenbaren. Wenn die mit der selbstbestimmten Preisgabe in Zusam-

---

[169] Im zugrunde liegenden Fall hatte das Gericht zu entscheiden, ob der Gebrauch eines bislang nicht zugelassenen Medikaments vom Right to Privacy erfasst und daher nur nach der Strict Scrutiny einschränkbar ist: Rutherford v. United States, 438 F.Supp. 1287, 1300 (W.D. Okla. 1977).

[170] *Mitchell*, Libertarian Paternalism Is an Oxymoron, 5.2002 FSU College of Law, Law and Economics Paper, 1, 19.

[171] Vgl.: *Allen*, Privacy Law and Society, ²2011, 240.

[172] Siehe oben Kapitel 3,C.I.2 und Kapitel 3,C.I.3.

menhang stehenden Gefahren jedoch noch nicht einmal in nennenswerter Weise verfassungsrechtlich geschützte Interessen tangieren, ist kein Bedrohungsszenario gegeben, das es ausnahmsweise nahelegen würde, einen Schutz der selbstbestimmt Handelnden vor sich selbst zu fordern.

Die Informationsfreiheit wird durch den Ersten Zusatzartikel geschützt und erfährt damit deutlich höheren Schutz als die informationelle Privatheit.[173] Das Ziel, den Bürgern ungehinderten Zugang zu Internetinformationsquellen zu gewährleisten, wäre damit jedenfalls ein näher liegendes Argument zur Rechtfertigung eines Schutzes vor sich selbst. Jedoch ist zu beachten, dass der Zugang zu Informationen durch informationelle Preisgabe nicht direkt verhindert wird, sondern es lediglich mittelbar zu einem beeinflussten Quellenangebot sowie zu Selbstzensur hinsichtlich der Quellenauswahl kommen kann. Die Bedrohungen sind damit zwar gegeben, erreichen jedoch keinen Gefährdungsgrad dramatischer Stufe. Ein solcher ließe sich vielleicht annehmen, wenn USA-weit alle Informationsquellen mit Zustimmung der Bürger abgeschafft werden sollten. Eine, im Vergleich dazu noch milde, Bedrohung durch informationelle Preisgabe erscheint nicht ausreichend, um einen Schutz der selbstbestimmt Handelnden vor sich selbst zu rechtfertigen.

Die Verhinderung selbstbestimmter Preisgabe zum Schutz der Preisgebenden ist daher nach geltendem Verfassungsverständnis unzulässig.

d) Moralische Pflicht zur Bewahrung informationeller Privatheit

Angesichts der Gefahren, die durch einen langfristigen Verlust an informationeller Privatheit ausgelöst werden können, scheint dieses Ergebnis problematisch. *Allen* schlägt daher eine moralische Obliegenheit zur Bewahrung informationeller Privatheit vor.[174] So, wie die Individuen durch den 13. Zusatzartikel daran gehindert seien, sich in Sklaverei zu begeben (was einen Schutz vor der Aufgabe dezisionaler Privatheit darstellt)[175], könnte ihnen auch die Bewahrung ihrer informationellen Privatheit obliegen.[176] Dieser Vergleich muss jedoch jedenfalls relativiert werden. Der 13. Zusatzartikel stellt den einzigen Fall einer echten Schutzpflicht in der U.S.-Verfassungsdogmatik dar.[177] Der Staat muss die Bürger davor schützen, sich einem Sklavenhalter unterzuordnen. *Allen* konstruiert jedoch wohl keine staatliche Pflicht zum Schutz informationeller Privatheit, sondern nur eine moralische Obliegenheit der Nutzer.

Sie mahnt, informationelle Privatheit (im Sinne der langfristigen Möglichkeit zur informationellen Selbstbestimmung) sei kein fakultatives Gut, wie ein zweites Haus

---

[173] Siehe oben Kapitel 3,C.I.4.

[174] Lesenswerte, kritische Antworten auf *Allens* Vorschläge bieten: *Moore*, Coercing Privacy and Moderate Paternalism, 13 Philosophy and Law (2013), 10 ff. und *Rössler*, Autonomy, Paternalism, and Privacy, 13 Philosophy and Law (2013), 14 ff.

[175] Zur Kategorie der dezisionalen Privatheit: siehe oben Kapitel 2,A.II.

[176] *Allen*, Coercing Privacy, 40 William and Mary L. Rev. (1999), 723, 728 f.

[177] Siehe oben Kapitel 5,B.

oder ein Anlagekonto.[178] Die Obliegenheit zur Privatheitswahrung beruhe originär darauf, dass die Individuen zum Schutz ihrer eigenen Interessen verpflichtet seien.[179] Sie müssten stets ihre rationalen Interessen an Sicherheit, Freiheit und günstigen Gelegenheiten fördern und zudem nach Selbstachtung, Würde und Integrität streben.[180] Die Preisgabe sensibler Daten zeige einen Mangel an Selbstachtung und behindere Freiheit und Autonomie, da dadurch zukünftige Optionen eingeschränkt würden.[181] Für das menschliche Leben sei nicht nur die Möglichkeit, sich für Privatheit zu entscheiden, bedeutend, sondern auch das tatsächliche Erleben von Privatheit.[182] Verstärkt würde diese Obliegenheit durch eine derivative Pflicht, die eigene Privatheit zu wahren, um fremde Interessen zu schützen: „My genome is also my siblings' genome, so I have an obligation to protect the privacy of my genome. My checking account number is also my husband's checking account number, so I have an obligation to protect the privacy of my checking account number. Among duties to others (family, friends, community) is a second-order duty to protect one's own informational privacy."[183]

Über die moralische Obliegenheit zur Bewahrung der Privatheit hinaus kann *Allen* sich auch staatliche Preisgabeverbote vorstellen. Neben zahlreichen entsprechenden Andeutungen[184] fordert sie derartige Schritte gelegentlich auch ausdrücklich.[185] Für zulässig erachtet sie jedenfalls „regulatory measures aimed at curbing

---

[178] *Allen*, Coercing Privacy, 40 William and Mary L. Rev. (1999), 723, 740.

[179] *Allen*, An Ethical Duty to Protect One's Own Informational Privacy?, 64 Alabama L. Rev. (2013), 845, 852.

[180] *Allen*, An Ethical Duty to Protect One's Own Informational Privacy? 64 Alabama L. Rev. (2013), 845, 854.

[181] *Allen*, Unpopular Privacy, 2011, 171 f. und *dies.*, An Ethical Duty to Protect One's Own Informational Privacy?, 64 Alabama L. Rev. (2013), 845, 857.

[182] *Allen*, Unpopular Privacy, 2011, 21.

[183] *Allen*, An Ethical Duty to Protect One's Own Informational Privacy?, 64 Alabama L. Rev. (2013), 845, 852, vgl.: 855, 862.

[184] „Government will have to intervene in private lives for the sake of privacy and values associated with it. Protecting privacy, however, rarely will require government to proscribe specific categories of conduct.": *Allen*, Coercing Privacy, 40 William and Mary L. Rev. (1999), 723, 755. In diese Richtung auch die Aussage: „[D]emocratic states […] could be justified in undertaking a rescue mission that includes enacting paternalistic privacy laws for the benefit of uneager beneficiaries.": *dies.*, Unpopular Privacy, 2011, XI; ebenso: „[L]egal policy makers […] must be open, in principle, to coercive privacy mandates that impose unpopular privacies on intended targets and beneficiaries.": *dies.*, Unpopular Privacy, 2011, XII; Schließlich merkt sie an „[W]e may even need laws that help create and preserve forms of privacy to which we may be unwisely indifferent": *dies.*, Unpopular Privacy, 2011, 196. Diese Aussagen werden jedoch eingeschränkt: „[G]overnment will not – and constitutionally perhaps cannot – do much to protect adults from voluntary conduct that erodes the taste for privacy and modest self-restraint. That important task is largely left to moral and ethical sectors": *dies.*, Unpopular Privacy, 2011, 194.

[185] „I continue to believe a just society can enact certain laws limiting the capacity of individuals to make choices about their own informational and physical privacy. [… I] claim that we should be open to laws that paternalistically intervene in the lives of adults (as well as children and youth), even when avoiding harms to third parties is not part of the picture.", *Allen*, Our Privacy Rights and Responsibilities, 13 Philosophy and Law (2013), 19, 23.

the culture of exposure for the sake of 'forcing' people to love privacy and live privately"[186] und somit wohl Maßnahmen, die sich als Entscheidungsarchitekturen bezeichnen lassen. Des Weiteren könnte sich aus der moralischen Obliegenheit der Individuen ein Anreiz für Unternehmen ableiten, im Rahmen ihrer Unternehmensverantwortung (der sogenannten Corporate Social Responsibility) privatheitsfördernd zu agieren.[187]

Doch selbst wenn eine moralische Obliegenheit zur langfristigen Wahrung der informationellen Privatheit besteht, kann diese nicht im verfassungsrechtlichen Sinn als Rechtfertigungsgrund für Freiheitsbeschränkungen dienen. Vielmehr kann und sollte diese Argumentation genutzt werden, um die aktuelle rechtspolitische Diskussion in den Vereinigten Staaten zur Verbesserung einfachgesetzlichen Privatheitsschutzes voranzutreiben. Sachgerecht erscheint es, ausgehend von *Allens* Argumentation, staatlicherseits zwar nicht die selbstbestimmte Preisgabe zu verhindern, aber jedenfalls Schritte zur Sicherung von Selbstbestimmung zu ergreifen.[188]

Für die vorliegende Analyse bleibt es aber dabei, dass der Schutz der selbstbestimmt Preisgebenden vor sich selbst de lege lata kein legitimer Eingriffszweck ist.

e) Unveräußerlichkeit informationeller Privatheit

Im Kontext des Schutzes vor sich selbst ist weiter an die Fälle ökonomischer Unveräußerlichkeit zu denken. Ist ein Gut per se unveräußerlich, ist davon auszugehen, dass die Verhinderung der Veräußerung gleichzeitig einen legitimen staatlichen Eingriffszweck darstellt.

Unveräußerlichkeit wird definiert als jede Eingrenzung der Übertragbarkeit, des Eigentums an oder der Nutzung einer Berechtigung.[189] Als Ausnahme vom marktwirtschaftlichen Grundgedanken der freien Veräußerlichkeit aller Güter werden bestimmte Güter als unveräußerlich eingestuft: Sie sollen nicht als Ware behandelt werden. Die Eigenschaft der Unveräußerlichkeit wird häufig genau den Gütern zugeschrieben, die für die Entwicklung der Persönlichkeit wichtig sind.[190] Wenn persönlichen Attributen, Beziehungen sowie philosophischen und moralischen Verpflichtungen ein ökonomischer Wert zugeordnet wird, wird die persönliche Identität untergraben.[191] Die genannten Beispiele betreffen moralische Werte und die Würde der Menschen. Der langfristige Verlust informationeller Privatheit birgt große Gefahren für die individuelle Persönlichkeitsentwicklung.[192] Daher wird vorgeschla-

---

[186] *Allen*, Coercing Privacy, 40 William and Mary L. Rev. (1999), 723, 753.

[187] *Allen*, An Ethical Duty to Protect One's Own Informational Privacy?, 64 Alabama L. Rev. (2013), 845, 850, 865.

[188] Siehe sogleich unten Kapitel 7,B.III.

[189] *Rose-Ackerman*, Inalienability and The Theory of Property Rights, 85 Columbia L. Rev. (1985), 931.

[190] *Radin*, Market-Inalienability, 100 Harvard L. Rev. (1987), 1849, 1903.

[191] *Radin*, Market-Inalienability, 100 Harvard L. Rev. (1987), 1849, 1905.

[192] Siehe oben Kapitel 3,A.II.3.

gen, auch Aspekte der informationellen Privatheit als unveräußerlich zu betrachten und damit ihre Aufgabe im Gegenzug zu einer wie auch immer gearteten Kompensation als unzulässig.[193] So könnte insbesondere die Einwilligung in bestimmte Datenerhebungen und -verwendungen unterbunden werden. Teilweise wird eine Unveräußerlichkeit bestimmter personenbezogener Daten angedacht, jedoch letztendlich nicht gefordert.[194] Anderenorts wird zwar gesehen, dass eine Unveräußerlichkeit dem Schutz individueller Würde zugutekommen kann, jedoch befürchtet, dass sie gleichsam dem Staat Kontrolle darüber geben würde, wie die Bürger mit ihrer informationellen Privatheit zu verfahren haben.[195] Jedenfalls hinsichtlich bestimmter enger Kategorien der Datenweitergabe scheint eine Unveräußerlichkeit denkbar. Als Beispiel genannt wird der Verkauf der Daten von Notaufnahmepatienten an Versicherungen oder Anwälte.[196] Die Vorschläge hinsichtlich der Unveräußerlichkeit von Privatheit scheinen jedoch primär in einer rechtspolitischen Forderung nach Schutz gegen ungewollte Kenntnisnahme durch private Dritte begründet, nicht jedoch auf den Schutz selbstbestimmt Preisgebender abzuzielen.

Neben den Überlegungen zur gänzlichen Unveräußerlichkeit bestimmter personenbezogener Daten wird zur Diskussion gestellt, dass bestimmte Rechte im Zusammenhang mit der Preisgabe personenbezogener Daten nicht veräußerlich sein sollen: So wird eine hybride Unveräußerlichkeit vorgeschlagen, die aus Beschränkungen der Verwendungs- und Übertragungsmöglichkeit der Daten und einem Opt-in zu jeder weiteren Verwendung oder Übertragung besteht.[197] Die Nutzer könnten ihre Daten zunächst übertragen, diese könnten jedoch nur für durch die Nutzer bestimmte Verwendungen genutzt werden. Den Preisgebenden müsste das Recht zustehen, alle weiteren Übertragungen oder die Nutzung durch Dritte zu blockieren, solange sie ihr Opt-in dazu nicht erteilen. Den Nutzern müssten überdies immer bestimmte Zugangs- und Berichtigungsrechte hinsichtlich ihrer personenbezogenen Daten bleiben.[198] Jedenfalls die Überlegungen zur eingeschränkten Unveräußerlichkeit ähneln dabei de facto der in Deutschland bestehenden Zweckbindung und den unverzichtbaren Betroffenenrechten (vgl. § 6 BDSG).

Die Idee, bereits die Preisgabe bestimmter Daten aufgrund einer Unveräußerlichkeit zu verhindern, hat sich in der Literatur nicht durchgesetzt. An einer entspre-

---

[193] *Cohen*, DRM and Privacy, 18 Berkeley Tech. L.J. (2003), 575, 608.

[194] *Cohen*, Examined Lives, 52 Stanford L. Rev. Online (2000), 1373, 1432 und *Schwartz*, Property, Privacy, and Personal Data, 117 Harvard L. Rev. (2004), 2055, 2074 ff.

[195] *Kang*, Information Privacy in Cyberspace Transactions, 50 Stanford L. Rev. Online (1998), 1193, 1266.

[196] *Kang*, Information Privacy in Cyberspace Transactions, 50 Stanford L. Rev. Online (1998), 1193, 1267, Fn. 302.

[197] *Schwartz*, Property, Privacy, and Personal Data, 117 Harvard L. Rev. (2004), 2055, 2094 ff. und *ders.*, Privacy Inalienability and the Regulation of Spyware, 20 Berkeley Tech. L.J. (2005), 1269, 1270 ff.

[198] *Kang*, Information Privacy in Cyberspace Transactions, 50 Stanford L. Rev. Online (1998), 1193, 1267, Fn. 302.

chenden Rechtsprechung fehlt es ebenfalls. Ein Schutz der Preisgebenden vor sich selbst kann daher – jedenfalls derzeit – nicht auf dem Umweg der Unveräußerlichkeit bestimmter personenbezogener Daten erfolgen.

f) Rechtfertigung der Sicherung der Selbstbestimmung

Etwas anderes könnte jedoch für Maßnahmen gelten, die lediglich der Sicherung der Selbstbestimmung dienen. Soweit solches Tätigwerden erforderlich ist, um die Selbstbestimmung zu gewährleisten (also die Unterstützung informationellen Selbstschutzes als milderes Mittel nicht ausreichend ist), dürfen nach deutschem Recht auch Entscheidungsarchitekturen eingesetzt werden. Ein erzwungener Schutz ist nach deutschem Recht unangemessen.[199]

Fraglich ist, ob und inwieweit nach US-Verfassungsrecht Maßnahmen zur Sicherung der Selbstbestimmung zulässig sind. Durch solche Maßnahmen kann sowohl explizite als auch implizite Preisgabe verhindert werden.

Zunächst kann durch Verhinderung expliziter (also bewusster und zielgerichteter) Preisgabe in die Redefreiheit der Preisgebenden eingegriffen werden. Voraussetzung für die Rechtfertigung solcher Maßnahmen ist das Verfolgen eines zwingenden staatlichen Zwecks. Die Verhinderung des Abgleitens in die fehlende Selbstbestimmung kann im staatlichen Interesse liegen. Allerdings besteht grundsätzlich die Vermutung dafür, dass Preisgebende selbstbestimmt handeln. Dies gilt auch im Grenzbereich zwischen Selbstbestimmung und fehlender Selbstbestimmung. So befasste sich der U.S. Supreme Court mit einem Gesetz, das vorsah, welchen Prozentsatz der eingeworbenen Spenden Benefizorganisationen maximal an professionelle Spendeneinwerber zahlen sollten.[200] Das Anwerben von Spendern ist Rede und genießt Schutz durch den Ersten Zusatzartikel. Durch das Gesetz sollte der Gefahr Rechnung getragen werden, dass Benefizorganisationen nicht selbstbestimmt entscheiden könnten, wie sie am effektivsten Spender werben können.[201] Die Verhinderung dieser Gefahren stellt jedoch keinen zwingenden staatlichen Zweck dar: „The First Amendment mandates that we presume that speakers, not the government, know best both what they want to say and how to say it. […] To this end, the government, even with the purest of motives, may not substitute its judgment as to how best to speak for that of speakers and listeners; free and robust debate cannot thrive if directed by the government.“[202] Obwohl die Gefahr bestand, dass die Rechtsträger ohne staatlichen Schutz ihre durch den Ersten Zusatzartikel geschützten Rechte (also das Einwerben von Spenden) nicht selbstbestimmt ausführen würden, durfte der Staat sie nicht vor sich selbst schützen. Solange keine Fremdbestimmung vorliegt, kann ein Eingriff in den Ersten Zusatzartikel der Preisgebenden

[199] Siehe oben Kapitel 6,A.I.1.d).
[200] Riley v. National Federation of the Blind of North Carolina, Inc., 487 U.S. 781, 781 (1988).
[201] Riley v. National Federation of the Blind of North Carolina, Inc., 487 U.S. 781, 790 (1988).
[202] Riley v. National Federation of the Blind of North Carolina, Inc., 487 U.S. 781, 791 (1988).

daher nicht gerechtfertigt werden. Eine Rechtfertigung der Verhinderung expliziter Preisgabe ist nicht möglich.

Die Verhinderung impliziter (also technisch im Hintergrund erfolgender und häufig unbewusster) Preisgabe ist am Rational-Basis-Test zu messen, die Maßnahme muss also lediglich in einem nachvollziehbaren Verhältnis zu einem legitimen Zweck stehen. Die Sicherung von Selbstbestimmung stellt einen legitimen Zweck dar. Sowohl die erzwungene Verhinderung impliziter Preisgabe als auch Entscheidungsarchitekturen, die implizite Preisgabe verhindern, stehen in einem nachvollziehbaren Verhältnis zu diesem Zweck und können gerechtfertigt werden. So wäre es beispielsweise jedenfalls mit den Rechten der Preisgebenden vereinbar, ihre Selbstbestimmung zu schützen, indem die Einwilligung zu Datenerhebungen als Opt-in gestaltet würde. Bevor verantwortliche Stellen Nutzerdaten erheben könnten, müssten die Nutzer dann zustimmen.

2. Rechtfertigung hinsichtlich der Redefreiheit der verantwortlichen Stellen

Allerdings könnte die Verhinderung von Preisgabe zum Schutz selbstbestimmt Preisgebender vor sich selbst in die Redefreiheit der verantwortlichen Stellen eingreifen und entsprechender Rechtfertigung bedürfen. Zu prüfen ist nur noch, ob implizite Preisgabe verhindert werden darf mit dem Ziel, die Selbstbestimmung der Preisgebenden zu wahren. In allen übrigen Fällen scheitert die Verhinderung selbstbestimmter Preisgabe zum Schutz der Preisgebenden bereits an den Rechten der Preisgebenden.

Durch die Verhinderung einer informationellen Preisgabe sind regelmäßig keine Privatinteressen der verantwortlichen Stellen betroffen, sondern kommerzielle Belange. Auch kommerzielle Rede findet Schutz durch den Ersten Zusatzartikel.[203] Sie kann nach dem sogenannten Central-Hudson-Test eingeschränkt werden, wenn ein substanzieller staatlicher Zweck verfolgt wird, die Maßnahme den Zweck direkt fördert und sie nicht umfangreicher als erforderlich ist („no more extensive than is necessary“).[204] Die Beweislast hierfür liegt – anders als bei der Erfüllung des Rational-Basis-Tests im Rahmen des prozessualen Due-Process-Schutzes – beim Staat.

Informationelle Privatheit kann dabei als entsprechender staatlicher Zweck dienen. Anerkannt sind beispielsweise der Schutz der Geheimhaltung von Finanzdaten[205] und der Schutz vor unerwünschter Kontaktaufnahme.[206] Dafür sollen jedoch, jedenfalls nach einem einflussreichen Obiter Dictum des Zehnten Circuit Court, enge Voraussetzungen gelten: „the government must show that the dissemination of

---

[203] St. Rspr., seit: Virginia State Board of Pharmacy v. Virginia Citizens Consumer Council, Inc., 425 U.S. 748, 758 ff. (1976).

[204] Central Hudson Gas & Elec. Corp. v. Public Service Commission of New York, 447 U.S. 557, 566 (1980).

[205] Individual Reference Services Group, Inc. v. FTC, 145 F.Supp.2d 6, 42 (D.D.C. 2001)

[206] Edenfield v. Fane, 507 U.S. 761, 769 (1993) und Florida Bar v. Went For It, Inc., 515 U.S. 618, 625 (1995).

the information desired to be kept private would inflict specific and significant harm on individuals, such as undue embarrassment or ridicule, intimidation or harassment, or misappropriation of sensitive personal information for the purposes of assuming another's identity. Although we may feel uncomfortable knowing that our personal information is circulating in the world, we live in an open society where information may usually pass freely. A general level of discomfort from knowing that people can readily access information about us does not necessarily rise to the level of a substantial state interest under *Central Hudson* for it is not based on an identified harm."[207] Voraussetzung ist also, dass der Staat die bedrohten signifikanten Privatheitsinteressen im Detail benennen kann. Das bloße Entstehen von Gefahren für die individuelle Persönlichkeitsentwicklung[208] wird häufig nicht die erforderliche Gefährdungsintensität erreichen.

Die Maßnahme muss weiter den Zweck direkt fördern. Die Anforderungen sind also deutlich höher als nach der Geeignetheitsprüfung im deutschen Verfassungsrecht. Dort bejaht die herrschende Ansicht die Geeignetheit bereits bei Vorliegen einer abstrakten Möglichkeit der Zweckerreichung.[209] Die vorzugswürdige, hier vertretene Ansicht fordert zudem einen nachvollziehbaren Wirkungszusammenhang.[210]

Auch die Prüfung, ob die Maßnahme nicht umfangreicher ist als erforderlich, geht über die deutsche Erforderlichkeitsprüfung hinaus. Während bei letzterer nur gefragt wird, ob ein gleich wirksames, aber weniger einschneidendes Mittel vorhanden ist, stellt das US-Recht auch die Frage, ob nicht insgesamt ein geringeres Schutzniveau gewählt werden kann.

Hinsichtlich der Rechtfertigungsanforderungen ist nach den Maßnahmenkategorien erzwungener Schutz (siehe a)), Unterstützung informationellen Selbstschutzes (siehe b)) und Entscheidungsarchitekturen zu unterscheiden (siehe c)). Im Anschluss wird ein Ausblick auf rechtspolitische Forderungen nach einer Absenkung des Schutzniveaus gegeben (siehe d)), bevor nach der Rechtfertigung im konkreten Fall gefragt wird (siehe e)).

a) Verhinderung der Preisgabe durch erzwungenen Schutz

Der Erste Zusatzartikel gewährleistet das Recht, ungehindert auf personenbezogene Daten Zugriff nehmen zu können, um diese für Direktmarketing auszuwerten. So entschied der U.S. Supreme Court, dass ein Gesetz, das den Verkauf, die Offenlegung und die Nutzung von Apotheken-Daten, die die Verschreibepraktiken einzelner Ärzte offenbaren, limitiert, am Recht der Arzneimittelhersteller aus dem Ersten Zusatzartikel zu messen ist. Die staatlichen Interessen daran, ärztliche Verschwie-

---

207 U.S. West, Inc. v. FCC, 182 F.3d 1224, 1235 (10th Cir. 1999) (Hervorhebung im Original).
208 Siehe oben Kapitel 3,A.II.
209 BVerfGE 100, 313 (373).
210 BVerfGE 107, 186 (197); siehe oben Kapitel 6,A.I.1.a).

genheit zu schützen, Ärzte vor Belästigung zu bewahren, ein gutes Arzt-Patienten-Verhältnis aufrechtzuerhalten und eine bessere Volksgesundheit bei Senkung der Gesundheitskosten zu erreichen, erkennt das Gericht zwar, sieht sie jedoch als durch das Gesetz nicht erreicht an.[211] Unter Anwendung des Central-Hudson-Tests fehlt es an der Erreichung des erforderlichen substanziellen staatlichen Zwecks: Das Gesetz ist verfassungswidrig. Das Gericht deutet sogar an, über den Central-Hudson-Test hinausgehen zu wollen, in dem es für inhaltsbezogene Einschränkungen kommerzieller Rede die Anwendung einer „heightened scrutiny" fordert.[212] Es bleibt jedoch unklar, was darunter zu verstehen ist, und ob diese Forderung Konsequenzen für die Rechtsentwicklung mit sich bringen wird.

Diese Rechtsprechung muss konsequenterweise auf die Verhinderung informationeller Preisgabe übertragen werden. Erhalten die verantwortlichen Stellen, gleich mit welchem primären Schutzziel, keine Daten, können sie diese nicht auswerten und als Folge keine personalisierten Angebote an die Nutzer richten. Verhindert der Staat unmittelbar durch erzwungenen Schutz die Preisgabe, schränkt er die Redefreiheit der verantwortlichen Stellen ein. Erzwungener Schutz bedarf daher der Rechtfertigung nach dem Central-Hudson-Test.

b) Verhinderung der Preisgabe durch Unterstützung informationellen Selbstschutzes

Ist die eingeschränkte Preisgabe hingegen nur mittelbare Folge der Unterstützung informationellen Selbstschutzes, sind es die Nutzer selbst, von denen das Unterbleiben der Preisgabe ausgeht. Ein Eingriff in die Rechte der verantwortlichen Stellen besteht dann, wie im deutschen Recht,[213] jedenfalls nicht darin, dass die verantwortlichen Stellen weniger Daten erhalten.

Dennoch können Maßnahmen zur Unterstützung informationellen Selbstschutzes am Ersten Zusatzartikel der verantwortlichen Stellen zu messen sein. Werden verantwortliche Stellen zum Bereitstellen von Informationen oder Warnungen gezwungen, liegt ein Fall der erzwungenen Rede (Compelled Speech) vor. Der Erste Zusatzartikel schützt nicht nur die Entscheidung, etwas zu sagen, sondern auch, etwas nicht zu sagen.[214] Auch erzwungene kommerzielle Rede genießt Schutz. Gerade weil der Schutz kommerzieller Rede durch den Ersten Zusatzartikel auf das Verbraucherinteresse an freiem Informationsfluss zurückgeführt wird,[215] ist das Schutzniveau für erzwungene kommerzielle Rede niedrig. Eine staatliche Maßnahme kann gerechtfertigt werden, wenn die Informationen, zu deren Übermittlung die

---

[211] Sorrell v. IMS Health Inc., 131 S.Ct. 2653, 2657 f. (2011).

[212] Sorrell v. IMS Health Inc., 131 S.Ct. 2653, 2657 (2011).

[213] Siehe oben Kapitel 6,A.I.2.

[214] Riley v. National Federation of the Blind of North Carolina, Inc., 487 U.S. 781, 797 (1988); st. Rspr., seit: West Virginia State Board of Education v. Barnette, 319 U.S. 624, 634 (1943).

[215] Virginia State Board of Pharmacy v. Virginia Citizens Consumer Council, Inc., 425 U.S. 748, 763 (1976).

Betroffenen gezwungen werden, nur faktisch und unkontrovers sind und die Informationsvorschrift in vernünftigem Zusammenhang mit dem staatlichen Zweck steht.[216] Mögliche staatliche Zwecke beschränken sich dabei nicht auf die Verhinderung der Irreführung der Verbraucher, sondern können verschiedene staatliche Informationsinteressen umfassen.[217] Ausgeschlossen ist der Zweck, lediglich die Neugierde der Bevölkerung zu befriedigen, ohne dass die betreffenden Fakten von irgendeiner Relevanz wären.[218]

Maßnahmen zur Unterstützung informationellen Selbstschutzes, die der Mitwirkung der verantwortlichen Stellen bedürfen, können daher gerechtfertigt werden, wenn sie sich nur auf unkontroverse Fakten, wie etwa technische Grundlagen der Preisgabe, erstrecken.

c) *Verhinderung der Preisgabe durch Entscheidungsarchitekturen*

Beim Einsatz von Entscheidungsarchitekturen ergibt sich ein Eingriff in die Redefreiheit der verantwortlichen Stellen nicht schon daraus, dass diese als Folge weniger Daten erhalten.

Abzustellen ist vielmehr darauf, dass die verantwortlichen Stellen im Regelfall zur Umsetzung der Entscheidungsarchitekturen verpflichtet werden. Geht die erzwungene Rede über die bloße Vermittlung von unkontroversen Fakten hinaus, genügt ein vernünftiger Zusammenhang zwischen der Maßnahme und dem staatlichen Zweck nicht, um den Eingriff zu rechtfertigen. Vielmehr findet der Central-Hudson-Test Anwendung.[219] Diese Schwelle ist erreicht, wenn die Betroffenen zur Vermittlung einer normativen Rede verpflichtet werden. Darunter wird eine Rede verstanden, die die Meinungen des Staates darüber transportiert, wie sich die Einzelnen zu verhalten haben.[220] Entscheidend ist dabei, ob der primäre Zweck das Vermitteln von Informationen ist, um eine informierte Entscheidung zu ermöglichen oder ob primär eine Verhaltensänderung herbeigeführt werden soll.[221]

---

[216] Zauderer v. Office of Disciplinary Counsel of Supreme Court of Ohio, 471 U.S. 626, 651 (1985).

[217] National Elec. Mfrs. Ass'n v. Sorrell, 272 F.3d 104, 115 (2d Cir. 2001) (Schutz menschlicher Gesundheit und der Umwelt); New York State Restaurant Ass'n v. New York City Bd. of Health, 556 F.3d 114, 136 (2d Cir. 2009) (Bekämpfung von Fettleibigkeit der Bevölkerung); ausführlich: *Keighley*, Can You Handle The Truth?, 15 J. of Constitutional L. (2012), 539, 556ff.; *Pomeranz*, Compelled Speech Under the Commercial Speech Doctrine, 12 J. of Health Care L. & Policy (2009), 159, 178; a.A.: R.J. Reynolds Tobacco Co. v. Food and Drug Admin., 696 F.3d 1205, 1213 (D.C. Cir. 2012).

[218] International Dairy Foods Ass'n v. Amestoy, 92 F.3d 67, 72f. (2d Cir. 1996).

[219] R.J. Reynolds Tobacco Co. v. Food and Drug Admin., 696 F.3d 1205, 1216ff. (D.C. Cir. 2012); *Rostron*, Pragmatism, Paternalism, and the Constitutional Protection of Commercial Speech, 37 Vermont L. Rev. (2013), 529, 571f.; in diese Richtung auch: *Willis*, When Nudges Fail, 80 Chicago L. Rev. (2013), 1115, 1212f.

[220] *Keighley*, Can You Handle The Truth?, 15 J. of Constitutional L. (2012), 539, 569.

[221] *Keighley*, Can You Handle The Truth?, 15 J. of Constitutional L. (2012), 539, 572, 574, 579.

Im Ausgangsfall R.J. Reynolds Tobacco Co. v. Food and Drug Admin. waren Grafiken auf Zigarettenschachteln keine reine Darstellung unkontroverser Fakten, sondern sollten gezielt Emotionen hervorrufen und so das Verhalten des Konsumenten ändern.[222] Einige der betreffenden Grafiken hatten sogar gar keinen Informationsgehalt, sondern zeigten beispielsweise nur das Bild eines Mannes, der ein T-Shirt mit der Aufschrift „I QUIT" trägt. Auch die Verpflichtung, auf jede Zigarettenschachtel die Telefonnummer „1-800-QUIT-NOW" einer Suchtberatungsstelle zu drucken, enthielt die Aufforderung, das Rauchen aufzugeben. Obwohl die Verpflichtung zur Abbildung von Grafiken häufig über das Vermitteln bloßer Informationen hinausgehen wird, muss dies nicht immer der Fall sein. Solange solche Abbildungen tatsächlich nur der besseren Darstellung von Informationen dienen, sind sie bei Vorliegen einer rationalen Basis rechtfertigbar.[223]

Auch Privatheitsschutz durch das verpflichtende Setzen von Defaults als weiteres Mittel der Entscheidungsarchitekturen unterfällt den Central-Hudson-Rechtfertigungsanforderungen, wie die Entscheidung U.S. West v. FCC des Zehnten Circuit Court aus dem Jahr 1999 zeigt. Im zugrunde liegenden Fall war die Federal Communications Commission mit der Ausgestaltung eines Gesetzes betraut worden, das die Einholung von Einwilligungen verlangt, bevor Telekommunikationsanbieter bestimmte Daten ihrer Kunden zu Marketingzwecken verwenden können. Die Federal Communications Commission hatte die Einwilligung als Opt-in gestaltet, verlangte also eine ausdrückliche Einwilligung. Das Gericht urteilte, dass das Marketing auf Basis der Nutzerdaten eine kommerzielle Rede darstellt, die durch die Redefreiheit der Telekommunikationsanbieter geschützt ist, sodass der Eingriff entsprechender Rechtfertigung bedarf. Der Schutz informationeller Privatheit kann ein staatliches Interesse sein, das grundsätzlich solche Eingriffe rechtfertigen kann. Jedoch war die Maßnahme im konkreten Fall nicht erforderlich (Narrowly Tailored), da das Gericht in wenig nachvollziehbarer Weise keine Nachweise dafür finden konnte, dass privatheitsbewusste Bürger nicht auch bei einer für die Anbieter weniger belastenden Opt-out-Regelung ihre Privatheit schützen würden.[224]

d) Rechtspolitische Forderungen nach Absenkung des Schutzniveaus

Die Rechte der verantwortlichen Stellen aus dem Ersten Zusatzartikel stellen häufig ein schwer überwindbares Hindernis beim Erlass datenschutzfreundlicher Gesetze dar. Dies stößt nicht nur international, sondern auch in den Vereinigten Staaten auf Kritik. Im Unterschied zu der bisherigen Rechtsprechung wird argumentiert, dass

---

[222] R.J. Reynolds Tobacco Co. v. Food and Drug Admin., 696 F.3d 1205, 1216 ff. (D.C. Cir. 2012).

[223] Dies wird bereits anerkannt durch: Zauderer v. Office of Disciplinary Counsel of Supreme Court of Ohio, 471 U.S. 626, 647 (1985): „The use of illustrations or pictures in advertisements […] may also serve to impart information directly."; *Keighley*, Can You Handle The Truth, 15 J. of Constitutional L. (2012), 539, 585.

[224] U.S. West, Inc. v. FCC, 182 F.3d 1224, 1239 (10th Cir. 1999).

einer kommerziellen Rede nur dann ein signifikanter Schutz durch den Ersten Zusatzartikel zuzusprechen sei, wenn ihr ein intrinsischer Wert für die Redefreiheit zukommt.[225] Im absoluten Regelfall seien die Schutzgründe aber derivativ, da eine kommerzielle Rede nur geschützt werde, um das Interesse der Zuhörer an der Kenntnisnahme der Rede abzusichern und ihnen die Möglichkeit zu geben, in Zukunft selbst zu sprechen. Es fehle hingegen an der Relevanz der kommerziellen Rede für die Persönlichkeitsentwicklung der Redenden. Bei der Bestimmung, ob einer kommerziellen Rede überhaupt Schutz durch den Ersten Zusatzartikel zukommt und wie hoch dieser Schutz ist, sei also ausschließlich auf die Relevanz der Interessen abzustellen, von denen sich der Schutzauftrag ableite. Damit fielen alle Maßnahmen, die den Schutz der Redefreiheit der Zuhörer bezwecken, von vornherein aus der Rechtfertigungsbedürftigkeit heraus. Demnach wären die Unterstützung informationellen Selbstschutzes und der Einsatz von Entscheidungsarchitekturen im Regelfall gar nicht an den Rechten der verantwortlichen Stellen aus dem Ersten Zusatzartikel zu messen. Ebenso erhielte das Recht der verantwortlichen Stellen auf die Datenerhebung zum Zweck, unerwünschte Werbung zu betreiben, keinen Schutz.

Dieser überzeugende Ansatz, der sich zudem dem europäischen Verständnis annähert, hat sich bislang jedoch noch nicht durchgesetzt. Die weitere Rechtsentwicklung bleibt abzuwarten.

e) Anwendung auf den konkreten Fall

Soweit es also in Betracht kommt, zur Sicherung der Selbstbestimmung implizite (also technisch im Hintergrund erfolgende, regelmäßig unbewusste) Preisgabe zu verhindern,[226] müssen diese Maßnahmen auch an den gemäß dem Ersten Zusatzartikel garantierten Rechten der verantwortlichen Stellen gemessen werden.

Maßnahmen zur Unterstützung informationellen Selbstschutzes erlegen den verantwortlichen Stellen häufig Informationspflichten auf. Solche erzwungene Rede ist mit deren Rechten aus dem Ersten Zusatzartikel vereinbar, wenn die Informationen, zu deren Übermittlung die Betroffenen gezwungen werden, nur faktisch und unkontrovers sind und die Informationsvorschrift im vernünftigen Zusammenhang zu dem staatlichen Interesse steht.[227] Derzeit beruht die Bereitstellung von Informationen über die Datenerhebung regelmäßig nicht auf gesetzlicher Anordnung, sondern auf Selbstverpflichtungen. Eine weiter gehende rechtliche Verpflichtung zur Offenlegung von mit der informationellen Preisgabe im Zusammenhang stehenden unkontroversen Fakten würde jedoch mit dem staatlichen Interesse an der Unterstüt-

---

[225] Siehe zu den folgende Ausführungen: *Wu*, The Commercial Difference, 18.5.2014, 1 ff. m. w. N.

[226] Siehe oben Kapitel 6,B.I.1.f).

[227] Zauderer v. Office of Disciplinary Counsel of Supreme Court of Ohio, 471 U.S. 626, 651 (1985).

zung informationellen Selbstschutzes in vernünftigem Zusammenhang stehen und wäre zulässig.[228]

Maßnahmen der Entscheidungarchitektur gehen hingegen über die Vermittlung unkontroverser Fakten hinaus und zwingen die verantwortlichen Stellen dazu, eine Botschaft zu übermitteln. Die Rechtfertigungsanforderungen des Central-Hudson-Tests finden Anwendung.[229] Eine Rechtfertigung ist demnach möglich, wenn ein substanzieller staatlicher Zweck verfolgt wird, die Maßnahme direkt den Zweck fördert und sie nicht umfangreicher als erforderlich ist.[230]

Der langfristige Privatheitsschutz kann einen substanziellen staatlichen Zweck darstellen, jedoch nur, wenn die Bedrohung präzise genug benannt werden kann und die erforderliche Intensität erreicht.[231] Durch eine nicht selbstbestimmte informationelle Preisgabe kann es zu Gefahren für die individuelle Persönlichkeitsentwicklung kommen. Deren Verhinderung kann an sich ein substanzieller staatlicher Zweck sein. Jedoch ist zu beachten, dass im Grenzbereich zwischen Selbst- und Fremdbestimmung keineswegs sicher ist, dass überhaupt eine nicht selbstbestimmte informationelle Preisgabe stattfinden wird. Weiter sind die Gefahren hypothetischer Natur, ihr Eintritt also nicht gewiss. Es bedarf daher im Einzelfall einer präzisen Darlegung, worin genau die zu verhindernden Gefahren bestehen und dass diese ausreichend gravierend sind. Gelingt dies, ist ein entsprechender staatlicher Zweck gegeben. Entscheidungsarchitekturen fördern diesen staatlichen Zweck auch unmittelbar. Dabei dürfen die Maßnahmen nicht umfangreicher als erforderlich sein. Ob dies der Fall ist, muss im Einzelfall geprüft werden. Die Unterstützung informationellen Selbstschutzes ist ein milderes Mittel, jedoch häufig weniger wirksam. Allerdings ist das US-Recht von dem Glauben an individuelle Verantwortlichkeit geprägt, sodass von den Einzelnen grundsätzlich erwartet wird, bei Kenntnis der relevanten Fakten eigenverantwortlich entscheiden zu können. Nur wenn davon auszugehen ist, dass andernfalls eine eigenverantwortliche Entscheidung im konkreten Fall nicht gelingt, sind Mittel der Entscheidungsarchitektur nicht umfangreicher als erforderlich.

Während es mit den Rechten der Nutzer vereinbar wäre, Einwilligungen zur Datenerhebung verpflichtend als Opt-in zu gestalten,[232] ließen sich solche Maßnahmen nicht mit der Redefreiheit der verantwortlichen Stellen vereinbaren. Das demonstriert die angesprochene Entscheidung U.S. West v. FCC des Zehnten Circuit Court, nach der eine Opt-in-Regelung hinsichtlich der Verwendung von Telekommunikationsdaten zu Marketingzwecken nicht erforderlich ist, da das Gericht keine Nach-

---

228 Als Vorbild dienen könnte beispielsweise § 13 Abs. 1 Satz 1 TMG.

229 R.J. Reynolds Tobacco Co. v. Food and Drug Admin., 696 F.3d 1205, 1216 ff. (D.C. Cir. 2012).

230 Central Hudson Gas & Elec. Corp. v. Public Service Commission of New York, 447 U.S. 557, 566 (1980).

231 U.S. West, Inc. v. FCC, 182 F.3d 1224, 1235 (10th Cir. 1999).

232 Siehe oben Kapitel 6,B.I.1.f).

weise dafür finden konnte, dass privatheitsbewusste Bürger nicht auch bei einer für die Anbieter weniger belastenden Opt-out-Regelung ihre Privatheit schützen würden.[233] Nur in sehr begrenzten Fällen können daher Entscheidungsarchitekturen mit den Rechten aus dem Ersten Zusatzartikel der verantwortlichen Stellen vereinbart werden.

Erzwungener Schutz zur Sicherung der Selbstbestimmung ist hingegen jedenfalls umfangreicher als erforderlich und verletzt die Redefreiheit der verantwortlichen Stellen.

Die bisher gewonnenen Ergebnisse lassen sich wie folgt zusammenfassen: Soweit eine staatliche Maßnahme Preisgabe beschneiden soll, die durch den Ersten Zusatzartikel oder die Due-Process-Klauseln geschützt ist, bedarf es der Rechtfertigung. Der Schutz der selbstbestimmt Preisgebenden vor sich selbst stellt im Regelfall keinen zulässigen staatlichen Eingriffszweck dar. Eine Rechtfertigung ist daher grundsätzlich nicht möglich. Zur Sicherung der Selbstbestimmung darf jedoch durch die Unterstützung informationellen Selbstschutzes und in sehr begrenzten Fällen durch Entscheidungsarchitekturen implizite Preisgabe verhindert werden.

II. Rechtfertigung des Schutzes nicht selbstbestimmt Preisgebender

Anders stellt sich die Situation dar, wenn die Preisgebenden nicht selbstbestimmt handeln.

1. Evaluationsmaßstäbe

Die für das deutsche Recht vorgenommene Kategorisierung der Situationen, in denen es an Selbstbestimmtheit fehlt,[234] erscheint auch für das US-Recht treffend. Demnach sind die fehlende Einsichtsfähigkeit und die fehlende Wahlmöglichkeit zu unterscheiden:

Fehlende Einsichtsfähigkeit kann vorliegen bei psychisch Kranken und geistig Behinderten sowie bei Minderjährigen (abgestuft je nach Alter).

Menschen, denen es aufgrund Krankheit oder Behinderung an Einsichtsfähigkeit fehlt (die also „incompetent" sind), dürfen vom Staat vor Selbstschädigung bewahrt werden. Während gesunde Grundrechtsträger nicht vor sich selbst geschützt werden dürfen, ist die Situation bei fehlender Einsichtsfähigkeit anders zu beurteilen, wie der U.S. Supreme Court ausführt: „This does not mean that an incompetent person should possess the same right, since such a person is unable to make an informed and voluntary choice to exercise that hypothetical right or any other right."[235]

---

[233] U.S. West, Inc. v. FCC, 182 F.3d 1224, 1239 (10th Cir. 1999). a.A.: *Wu*, The Commercial Difference, 18.5.2014, 25; siehe oben Kapitel 6,B.I.2.

[234] Siehe oben Kapitel 5,A.VI.

[235] Cruzan by Cruzan v. Director, Missouri Dept. of Health, 497 U.S. 261, 262 (1990); vgl.: Bouvia v. Superior Court, 179 Cal. App.3d 1127, 1137 ff. (Cal. App. 2. Dist. 1986).

Als Beispiel für den Schutz Minderjähriger kann der Children's Online Privacy Protection Act dienen.[236] Unter anderem verboten ist nach dessen § 6502 das Sammeln personenbezogener Daten von unter Dreizehnjährigen ohne Vorliegen einer nachprüfbaren Einwilligung eines Erziehungsberechtigten. Darüber hinaus ist es selbst bei Vorliegen einer Einwilligung des Erziehungsberechtigten verboten, die Teilnahme eines Kindes an Gewinnspielen und Ähnlichem von der Preisgabe nicht erforderlicher personenbezogener Daten abhängig zu machen. Zudem kann von der Einhaltung gesetzlich festgelegter besonderer Sicherheitsstandards auch bei Vorliegen einer Einwilligung des Erziehungsberechtigten nicht abgesehen werden.

An Wahlmöglichkeiten fehlt es, wenn die Auswahl von vorneherein durch faktische Zwänge (also Machtdisparität oder das Angewiesensein auf ein bestimmtes Produkt) oder unverschuldete mangelnde Informiertheit auf sehr wenige Optionen oder nur eine limitiert ist.

Schutz vor faktischen Zwängen bietet die Unconscionability-Doktrin, nach der Verträge nicht durchsetzbar sind, die so unfair und einseitig sind, dass kein vernünftiger Mensch ihnen zugestimmt hätte, es also an jeder „meaningful choice" fehlte.[237] Ob dies der Fall war, muss unter Berücksichtigung aller Umstände der Transaktion untersucht werden. Häufig indiziert ein eklatantes Verhandlungsungleichgewicht eine mangelnde Selbstbestimmung. Auch die Umstände des Vertragsabschlusses, wie das Bildungsniveau der Vertragsparteien, das Verstecken wichtiger Informationen in Kleingedrucktem oder ein irreführendes Verhalten der anderen Partei spielen eine Rolle.[238]

Auch gibt es Fälle, in denen faktische Zwänge hinsichtlich der Preisgabe typisiert angenommen und die Betroffenen davor geschützt werden. So ist es nach dem Employee Polygraph Protection Act (EPPA)[239] Arbeitgebern, von wenigen Ausnahmen abgesehen, verboten, die Ergebnisse von Lügendetektortests, denen sich Bewerber oder Arbeitnehmer freiwillig unterzogen haben, anzunehmen, zu verwenden, sich auf diese zu beziehen oder darauf basierende Nachforschungen anzustellen. Den Bewerbern oder Arbeitnehmern, die die Wahrheit sagen, geht damit die Möglichkeit verloren, durch einen solchen Test ihre Unschuld zu beweisen. Dieses Interesse der Betroffenen wird in der Rechtsordnung durchaus anerkannt, jedoch, soweit ersichtlich, nur im Hinblick auf das Recht, im Strafverfahren ihren Aussagen durch Zustimmung zu einem Lügendetektortest mehr Glaubwürdigkeit zu verleihen.[240] Im Arbeitskontext wird jedoch ein Mangel an Selbstbestimmtheit angenommen und die Bewerber und Arbeitnehmer werden davor geschützt.

---

[236] 15 U.S.C. § 6501 ff., umgesetzt durch die Children Online Privacy Protection Rule, 16 C.F.R. § 312, geändert am 17.1.2013; zu den Änderungen: *Federal Trade Commission*, FTC Strengthens Kids' Privacy, Gives Parents Greater Control Over Their Information By Amending Children's Online Privacy Protection Rule, 19.12.2012.

[237] Vgl. § 2-302 U.C.C.

[238] Williams v. Walker-Thomas Furniture Co., 350 F.2d 445, 449 (1965).

[239] 29 U.S.C. 2001 ff.

[240] Com. v. Moynihan, 376 Mass. 468, 478 f. (Mass. 1978).

In vergleichbarer Weise ist es Krankenversicherern und Arbeitgebern nach dem Genetic Information Nondiscrimination Act verboten, die Preisgabe von Gendaten Betroffener zu erfragen oder zu verlangen. Auch wenn sie diese Daten auf anderem Wege erhalten, dürfen die Daten nicht verwendet werden.[241]

2. Rechtfertigung hinsichtlich der Rechte der Preisgebenden

Fraglich ist zunächst, ob der Schutz der nicht selbstbestimmt Preisgebenden vor sich selbst an deren Rechten zu messen ist. Dies ist jedoch zu verneinen. Werden nicht selbstbestimmt Preisgebende an der Preisgabe gehindert, liegt, wie auch im deutschen Recht,[242] kein Eingriff in ihre Rechte vor.[243] Den Preisgebenden wird keine Selbstbestimmung genommen, sondern Schutz vor Fremdbestimmung durch die verantwortlichen Stellen gegeben. Eine Rechtfertigung hinsichtlich der Rechte der Preisgebenden ist daher entbehrlich.

3. Rechtfertigung hinsichtlich der Redefreiheit der verantwortlichen Stellen

Notwendig bleibt jedoch die Rechtfertigung hinsichtlich der Redefreiheit der verantwortlichen Stellen.

Da nicht selbstbestimmt Preisgebende gerade nicht selbstbestimmt entscheiden können, tragen zu ihrem Schutz die Unterstützung informationellen Selbstschutzes sowie Entscheidungsarchitekturen keine Früchte. Einzig wirksames Mittel ist ein erzwungener Schutz.

Erzwungener Schutz zur Verhinderung nicht selbstbestimmter informationeller Preisgabe ist, soweit damit die verantwortlichen Stellen keine oder nur eingeschränkte Daten erhalten, an deren Rechten aus dem Ersten Zusatzartikel zu messen. Da sie keine Daten erlangen, um auf dieser Basis die Nutzer mit personalisierten Angeboten versorgen zu können, ist ihr Interesse an der Durchführung kommerzieller Rede beeinträchtigt. Eingriffe können nach dem Central-Hudson-Test gerechtfertigt werden, wenn ein substanzieller staatlicher Zweck verfolgt wird, die Maßnahme direkt diesen Zweck fördert und sie nicht umfangreicher als erforderlich ist.[244] Der Schutz der nicht selbstbestimmt Preisgebenden ist ein substanzieller staatlicher Zweck, dessen Verwirklichung durch die Erzwingung von Schutz direkt gefördert wird. Im Einzelfall muss sichergestellt werden, dass sich der Schutz auf nicht selbstbestimmt Preisgebende beschränkt. Nur wenn dies der Fall ist, kann die Maßnahme gerechtfertigt werden.

---

241 Durch den Genetic Information Nondiscrimination Act wurde eine Vielzahl einzelner Gesetze geändert. Eine Übersicht ist abrufbar unter: https://www.govtrack.us/congress/bills/110/hr493/text.

242 Siehe oben Kapitel 6,A.II.1.

243 Cruzan by Cruzan v. Director, Missouri Dept. of Health, 497 U.S. 261, 262 (1990).

244 Central Hudson Gas & Elec. Corp. v. Public Service Commission of New York, 447 U.S. 557, 566 (1980).

Zusammenfassend hat sich gezeigt, dass der Schutz nicht selbstbestimmt Preisgebender nicht in deren Rechte eingreift und damit lediglich an der Redefreiheit der verantwortlichen Stellen zu messen ist. Nur ein erzwungener Schutz stellt ein wirksames Mittel zum Schutz der nicht selbstbestimmt Preisgebenden dar. Dieser kann gerechtfertigt werden, wenn er nicht umfangreicher als erforderlich ist.

III. Rechtfertigung des Schutzes von Allgemeinwohlbelangen

Schließlich ist zu prüfen, ob die Verhinderung informationeller Preisgabe zum Schutz von Allgemeinwohlbelangen gerechtfertigt werden kann.

1. Rechtfertigung hinsichtlich der Rechte der Preisgebenden

Die Verhinderung informationeller Preisgabe könnte in die Redefreiheit der Preisgebenden (siehe a)) eingreifen und gegen prozessuale Due-Process-Anforderungen (siehe b)) verstoßen.

a) Rechtfertigung hinsichtlich der Redefreiheit

Die Verhinderung expliziter (also bewusster und zielgerichteter) informationeller Preisgabe stellt einen Eingriff in die Redefreiheit dar. Zur Rechtfertigung wird der strenge Rechtfertigungsstandard Strict Scrutiny angewandt, es muss also ein zwingender staatlicher Zweck verfolgt werden, der nicht auch durch weniger restriktive Mittel gleich wirksam erreicht werden kann.[245] Ein entsprechender staatlicher Zweck liegt vor, wenn sich die Allgemeinwohlbelange in der Abwägung gegen die Redefreiheit der Preisgebenden durchsetzen.

Zunächst ist fraglich, ob der Schutz Dritter einen zwingenden staatlichen Zweck darstellt. Dagegen könnte sprechen, dass die US-Grundrechtsdogmatik – anders als das Grundgesetz, das eine gleichberechtigte Abwägung zwischen den Rechten der Preisgebenden und den Rechten Dritter vorsieht – Privatheitsinteressen regelmäßig hinter dem durch den Ersten Zusatzartikel geschützten freien Fluss von Informationen zurücktreten lässt.[246] Plakativ formulierte U.S. Supreme Court *Justice Brandeis*: „sunlight is the most powerful of all disinfectants.“[247]

Das Ungleichgewicht zwischen der Redefreiheit und den Privatheitsinteressen Anderer spiegelt sich auch in der Zivilrechtsordnung wieder: Das Common Law kennt vier deliktsrechtliche Privatheitsansprüche (sogenannte Privacy Torts), in denen sich verschiedene Formen von Privatheitsinteressen der Dritten gegen die Rede-

---

[245] Reno v. American Civil Liberties Union, 521 U.S. 844, 874 (1997).

[246] *Buchner*, Informationelle Selbstbestimmung im Privatrecht, 2006, 20 ff., 83 ff.; *Post*, Yellow Press and Privacy, GRUR Int 2006, 283, 292; *Whitman*, The Two Western Cultures of Privacy, 113 Yale L. J. (2004), 1151, 1209 und *Wittern*, Das Verhältnis von Right of Privacy und Persönlichkeitsrecht zur Freiheit der Massenmedien, 2004, 270 ff.

[247] Berühmt geworden durch: New York Times Co. v. Sullivan, 376 U.S. 254, 305 (1964) (*Goldberg*, *Douglas*, *JJ.*, concurring).

freiheit der Preisgebenden durchsetzen. *Prosser* brachte im Jahr 1960 durch Analyse von mehr als dreihundert Gerichtsentscheidungen die unterschiedlichen Rechtsprechungslinien in ein System. In seinem Artikel „Privacy“[248] analysiert er die bis dahin vorhandene Rechtsprechung und fasst sie in vier Kategorien zusammen: die Veröffentlichung privater Fakten,[249] das Eindringen in die Zurückgezogenheit,[250] falsche Behauptungen (aufzuteilen in Defamation, False Light und Infliction of Emotional Distress)[251] sowie die Anmaßung eines Namens oder einer Eigenschaft[252]. Diese Kategorisierung wird im Restatement of Torts (Second) des American Law Institutes annähernd übernommen und bildet die Grundlage für die im Wesentlichen bundesstaatliche Privatheits-Rechtsprechung. Ein generelles Recht auf informationelle Privatheit ist nicht erfasst und die Gerichte zeigen sich sehr zurückhaltend hinsichtlich einer erweiternden Auslegung der vier Kategorien.[253]

Weitere Beispiele, in denen sich Privatheitsinteressen gegen die Redefreiheit durchsetzen, sind berufliche Verschwiegenheits- und Geheimhaltungspflichten etwa von Ärzten oder Anwälten.[254]

Es ist anerkannt, dass der Schutz der Rechte Dritter ein zwingendes staatliches Interesse darstellt, soweit die informationelle Preisgabe einen der vier Privacy Torts erfüllt oder gegen Verschwiegenheits- und Geheimhaltungspflichten verstößt. Dann ist auch erzwungener Schutz rechtfertigbar, soweit andere Mittel nicht gleich wirksam sind. Von diesen Ausnahmen abgesehen werden die Gerichte jedoch im Zweifel die Rechte der Preisgebenden höher gewichten als die Rechte der betroffenen Dritten.

Soweit Dritte von der Preisgabe gar nicht betroffen sind, sondern nur abstrakte Allgemeinwohlbelange wie der gesellschaftliche Fortschritt oder die Demokratie, wird die Rechtfertigung von Maßnahmen zur Verhinderung der Preisgabe noch unwahrscheinlicher. Zwar genießen der gesellschaftliche Fortschritt und die Funktionsfähigkeit der Demokratie verfassungsrechtlichen Stellenwert. Doch besteht gerade keine verfassungsrechtliche Pflicht der Einzelnen, einen Beitrag hierzu zu

---

248 *Prosser*, Privacy, 48 California L. Rev. (1960), 383 ff.

249 Restatement (2d) Torts, § 652D; ausführlich: *Solove/Schwartz*, Information Privacy Law, ³2009, 105 ff.

250 Restatement (2d) Torts, § 652B; ausführlich: *Solove/Schwartz*, Information Privacy Law, ³2009, 78 ff.

251 Restatement (2d) Torts, § 652E; ausführlich: *Solove/Schwartz*, Information Privacy Law, ³2009, 202 ff.

252 Restatement (2d) Torts, § 652C; ausführlich: *Solove/Schwartz*, Information Privacy Law, ³2009, 205 ff.

253 „Appellants have requested that this court make new law by expanding the present concept of invasion of privacy to include the practice complained of here [Verkauf von Namen und Adressen an Werbefirmen]. It is not within our province to create a specific right which is not recognized at common law. The forum to which appellants should look is the legislature because the appropriate remedy in this situation is the creation of a statutory right.“: Shibley v. Time, 45 Ohio App. 2d 69, 73 (Ohio App. 1975).

254 Einen Überblick bietet: *Allen*, An Ethical Duty to Protect One's Own Informational Privacy?, 64 Alabama L. Rev. (2013), 845, 847.

leisten. Eine solche darf auch nicht durch die Hintertür eingeführt werden durch eine Pflicht, um dieser Interessen willen auf informationelle Preisgabe zu verzichten. Angesichts des hohen Stellenwerts der Redefreiheit ist es schwerlich vorstellbar, dass ein staatliches Interesse am Schutz von abstrakten Allgemeinwohlbelangen die Relevanz eines zwingenden staatlichen Zweckes erreicht. Eine Verhinderung expliziter informationeller Preisgabe zum Schutz abstrakter Allgemeinwohlbelange ist daher nicht möglich.

b) Rechtfertigung hinsichtlich des prozessualen Due-Process-Standards

In den nicht durch die Redefreiheit geschützten Fällen – also der Verhinderung expliziter Preisgabe durch Entscheidungsarchitekturen sowie der Verhinderung impliziter Preisgabe durch erzwungenen Schutz sowie Entscheidungsarchitekturen – kann informationelle Preisgabe nach dem Rational-Basis-Test verhindert werden, wenn die Maßnahme in einem nachvollziehbaren Verhältnis zu einem legitimen Zweck steht.

Der Schutz der informationellen Privatheit Dritter sowie abstrakter Allgemeinwohlbelange stellt einen legitimen Zweck dar. Je nach Situation können sowohl erzwungener Schutz als auch Entscheidungsarchitekturen in einem nachvollziehbaren Verhältnis zu diesem Zweck stehen und daher gerechtfertigt werden.

2. Rechtfertigung hinsichtlich der Redefreiheit der verantwortlichen Stellen

Weiter müssen Maßnahmen zum Schutz von Allgemeinwohlbelangen mit der Redefreiheit der verantwortlichen Stellen vereinbar sein.

Fraglich ist zunächst, ob Preisgabe zum Schutz Dritter verhindert werden darf. Zur Rechtfertigung von erzwungenem Schutz und Entscheidungsarchitekturen muss der Central-Hudson-Standard erfüllt werden. Der Schutz derjenigen, deren Belange sich tatsächlich gegen die Redefreiheit der Preisgebenden durchsetzen, ist ein entsprechender Zweck. Durch erzwungenen Schutz sowie Entscheidungsarchitekturen wird der Zweck auch direkt gefördert. Es ist das im Einzelfall am wenigsten umfangreiche Mittel auszuwählen, wobei ein erzwungener Schutz häufig das einzig wirksame Mittel sein wird. Die Unterstützung informationellen Selbstschutzes mit dem Zweck, Dritte zu schützen, bedarf nur dann der Rechtfertigung, wenn die verantwortlichen Stellen zur Umsetzung verpflichtet werden, indem ihnen insbesondere Informationspflichten auferlegt werden. Die Maßnahme kann dann gerechtfertigt werden, wenn die Informationen, zu deren Übermittlung die Betroffenen gezwungen werden, nur faktisch und unkontrovers sind und die Informationsvorschrift im vernünftigen Zusammenhang mit dem staatlichen Interesse steht.[255] Zu beachten ist allerdings, dass Informationspflichten, die verantwortliche Stellen

255 Zauderer v. Office of Disciplinary Counsel of Supreme Court of Ohio, 471 U.S. 626, 651 (1985).

den Preisgebenden gegenüber erfüllen müssen, nur selten geeignet sein werden, den Schutz der durch die Preisgabe beeinträchtigten Dritten zu erreichen. Entsprechende Konstellationen lassen sich jedoch denken („Lieber Nutzer, auf dem Foto sind auch weitere Personen zu sehen, deren Rechte verletzt werden könnten.“). Soweit die Informationspflichten zum Unterbleiben der Preisgabe führen können, stehen sie in einem vernünftigen Zusammenhang mit dem staatlichen Zweck, die informationelle Privatheit der Dritten zu schützen.

Darüber hinaus ist zu analysieren, ob die Verhinderung von Preisgabe zum Schutz von gesellschaftlichem Fortschritt und der Demokratie mit den gemäß dem Ersten Zusatzartikel geschützten Rechten der verantwortlichen Stellen zu vereinbaren ist. Zur Rechtfertigung von einem erzwungenen Schutz und von Maßnahmen der Entscheidungsarchitektur müsste der Central-Hudson-Standard erfüllt sein, wobei abstrakte Gefahren jedoch nicht ausreichen. Der Schutz des gesellschaftlichen Fortschritts sowie der Demokratie kann an sich ein substanzieller staatlicher Zweck sein. Jedoch ist die Wahrscheinlichkeit des Eintritts der dargestellten Gefahren[256] nicht konkret genug, als dass deren Verhinderung als substanzieller staatlicher Zweck gewertet werden könnte. Auch obliegt den verantwortlichen Stellen keine Pflicht, einen Beitrag zu gesellschaftlichem Fortschritt oder der Demokratie zu leisten. Eine Rechtfertigung ist daher nicht möglich.

Etwas anders gilt für die Unterstützung informationellen Selbstschutzes. Soweit den verantwortlichen Stellen Pflichten zur Wiedergabe faktischer und unkontroverser Informationen auferlegt werden, sind diese gerechtfertigt, wenn die Pflichten in einem vernünftigen Zusammenhang mit dem staatlichen Zweck stehen. Informationspflichten können insgesamt zu einem Rückgang der Preisgabe führen und damit der Allgemeinheit zugutekommen. Auch könnte ausdrücklich über die Gefahren aufgeklärt werden, die die Preisgabe für die Allgemeinheit herbeiführen kann („Lieber Nutzer, wenn Du Deine politische Orientierung in Deinem Profil im sozialen Netzwerk angibst, kann das dazu führen, dass Du von Deiner Umwelt auch dann noch mit ihr assoziiert wirst, wenn Du sie in der Zukunft änderst.“). Dadurch können die Nutzer, jedenfalls theoretisch, von der Preisgabe abgehalten werden. Zum Schutz abstrakter Allgemeinwohlbelange lassen sich Informationspflichten daher rechtfertigen. Ob diese tatsächlich ausreichenden Erfolg versprechen, ist im Einzelfall vom Gesetzgeber zu entscheiden.

C. Vergleich

Trotz identischer Gefahrenlage und eines übereinstimmenden Katalogs realiter möglicher Maßnahmen zeigen sich Unterschiede darin, inwieweit eine Verhinderung informationeller Preisgabe in Deutschland und in den Vereinigten Staaten verfassungsrechtlich zulässig ist.

---

[256] Siehe oben Kapitel 3,A.III.2 und Kapitel 3,A.III.3.

I. Evaluationsmaßstäbe

Die zu berücksichtigenden verfassungsmäßigen Rechte unterscheiden sich in beiden Rechtsordnungen. Es wird ein funktionaler Ansatz gewählt, um die Rechte miteinander vergleichen zu können, die jeweils bei der Verhinderung informationeller Preisgabe zu berücksichtigen sind. Entscheidend ist die Funktion der Regel, abgestellt wird also nicht auf den abstrakten Wortlaut, sondern auf die Rechtswirklichkeit.[257] Dabei zeigt sich:

– In beiden Rechtsordnungen greifen Maßnahmen zur Unterstützung informationellen Selbstschutzes nicht in die Rechte der Preisgebenden ein.
– In Deutschland werden erzwungener Schutz und Entscheidungsarchitekturen einheitlich am Recht auf informationelle Selbstbestimmung der Preisgebenden gemessen. Unerheblich ist, ob explizite (also bewusste und zielgerichtete) oder implizite (also technisch im Hintergrund laufende, häufig unbewusste) Preisgabe verhindert werden soll. In seltenen Fällen besteht auch Schutz durch die Meinungs-, Informations- oder Berufsfreiheit.
  Dagegen ist in den USA die erzwungene Verhinderung expliziter Preisgabe an der schwer einschränkbaren Redefreiheit zu messen, während in allen übrigen Fällen nur der niedrige prozessuale Due-Process-Schutz greift. Die Verhinderung expliziter Preisgabe durch erzwungenen Schutz ist daher in den USA weitaus schwieriger rechtfertigbar als in Deutschland, während alle anderen Maßnahmen deutlich einfacher zu rechtfertigen sind.
– Alle Maßnahmen sind jedoch zusätzlich an den Rechten der verantwortlichen Stellen zu messen. In Deutschland ist in erster Linie die Berufsfreiheit einschlägig, daneben unter Umständen noch die Eigentumsgarantie, die Meinungsfreiheit und subsidiär die wirtschaftliche Betätigungsfreiheit.
  In den Vereinigten Staaten hingegen ist nur die schwer einschränkbare Redefreiheit betroffen. Außer im Fall bloßer Unterrichtungsvorschriften ist die Hürde in den Vereinigten Staaten damit ungleich höher als nach dem Grundgesetz.

II. Analyse

Bei der Anwendung des dargestellten verfassungsrechtlichen Rahmens auf die verschiedenen Konstellationen der Verhinderung informationeller Preisgabe zeigt sich:

– Sollen selbstbestimmt Preisgebende vor sich selbst geschützt werden, dürfen in beiden Rechtsordnungen keine Maßnahmen ergriffen werden, es sei denn, sie dienen gerade der Herstellung oder Erhaltung der Selbstbestimmung.
  Zur Sicherung der Selbstbestimmung darf in Deutschland explizite und implizite Preisgabe verhindert werden, indem informationeller Selbstschutz unterstützt wird und, soweit erforderlich, Entscheidungsarchitekturen angewandt werden.[258]

---

[257] Zur Methode, siehe oben: Kapitel 3,D.
[258] Die zulässigen Konstellationen lassen sich wie folgt illustrieren:

In den USA darf lediglich versucht werden, die Nutzer durch die Unterstützung informationellen Selbstschutzes und, soweit erforderlich, durch Entscheidungsarchitekturen von impliziter Preisgabe abzuhalten.
Die Möglichkeiten zur Sicherung der Selbstbestimmung sind damit in Deutschland weiter als in den Vereinigten Staaten, da sie sich in den USA auf die Verhinderung impliziter Preisgabe beschränken.

– Der Schutz nicht selbstbestimmt Preisgebender greift nicht in deren Rechte ein und ist in beiden Rechtsordnungen lediglich an den Rechten der verantwortlichen Stellen zu messen. Zum Schutz nicht selbstbestimmt Preisgebender dürfen alle Maßnahmen ergriffen werden, wobei erzwungener Schutz regelmäßig das einzig wirksame Mittel ist. Ist nicht sicher, ob eine Preisgabe selbstbestimmt oder nicht selbstbestimmt erfolgt, kann typisierend eine fehlende Selbstbestimmung angenommen werden. Die rechtlichen Möglichkeiten zur Verhinderung nicht selbstbestimmter Preisgabe sind also in beiden Ländern vergleichbar.
– Wird der Schutz von Allgemeinwohlbelangen bezweckt, zeigen sich erhebliche Unterschiede:
Dienen die Interventionen dem Schutz Dritter, können in Deutschland nach Herstellung praktischer Konkordanz mit den Rechten der Preisgebenden Maßnahmen aus allen drei Kategorien gerechtfertigt sein. Dabei können die konkurrierenden Rechte als gleichrangig angesehen werden. Regelmäßig wird erzwungener Schutz das einzig wirksame Mittel sein.
In den Vereinigten Staaten lassen sich erzwungener Schutz und Entscheidungsarchitekturen nur dann rechtfertigen, wenn sich die Rechte Dritter tatsächlich gegen die Redefreiheit der Preisgebenden durchsetzen. Aufgrund der herausragenden Bedeutung der Redefreiheit beschränkt sich dies jedoch auf Einzelfälle. Nur die Unterstützung informationellen Selbstschutzes kann problemlos gerechtfertigt werden.
Die Verhinderung von Preisgabe zum Schutz Dritter ist somit in Deutschland deutlich einfacher möglich als in den USA.
In Deutschland lassen sich zum Schutz abstrakter gesellschaftlicher Belange die Unterstützung informationellen Selbstschutzes sowie, wenn erforderlich, Entscheidungsarchitekturen rechtfertigen, nicht aber erzwungener Schutz. Soweit dies möglich ist, ist jedoch von einem Eingriff abzusehen, indem die Maßnahmen

---

– „Lieber Nutzer, wenn Du den Post veröffentlichst, kann es sein, dass er dauerhaft im Internet auffindbar ist.“ (Verhinderung expliziter Preisgabe durch informationellen Selbstschutz),
– „Lieber Nutzer, wenn Du Deine Einwilligung zur Datenerhebung erteilst, kann es sein, dass Persönlichkeitsprofile von Dir erstellt werden.“ (Verhinderung impliziter Preisgabe durch informationellen Selbstschutz),
– „Lieber Nutzer, der Post wird erst in zehn Sekunden veröffentlicht, um Dir Bedenkzeit und die Möglichkeit zur Abänderung zu geben.“ (Verhinderung expliziter Preisgabe durch Entscheidungsarchitektur),
– „Lieber Nutzer, wenn Du wirklich willst, dass Cookies gesetzt werden, willige ausdrücklich ein.“ (Verhinderung impliziter Preisgabe durch Entscheidungsarchitektur).

entweder vom Staat selbst durchgeführt oder die verantwortlichen Stellen durch Anreize zur Implementierung bewegt werden.
In den Vereinigten Staaten ist zum Schutz abstrakter gesellschaftlicher Belange lediglich die Unterstützung informationellen Selbstschutzes zulässig, da dem Einsatz von Entscheidungsarchitekturen die Redefreiheit der verantwortlichen Stellen entgegensteht.
Auch zum Schutz gesellschaftlicher Belange können damit in Deutschland weitergehende Maßnahmen ergriffen werden als in den USA.

Die unterschiedlichen Möglichkeiten zur Verhinderung informationeller Preisgabe in Deutschland und den Vereinigten Staaten lassen sich maßgeblich auf drei Unterschiede im Grundrechtsverständnis zurückführen:

Zunächst kommt der informationellen Privatheit der Preisgebenden ein grundsätzlich verschiedener Stellenwert zu. Während das deutsche Verfassungsrecht ihr große Bedeutung zumisst, erfährt die informationelle Privatheit derjenigen, die Daten selbst im Internet preisgeben, in den USA fast keinen Schutz.[259] Entsprechend sind auch Maßnahmen, die die informationelle Privatheit schützen möchten, indem sie informationelle Preisgabe verhindern, in Deutschland leichter zu rechtfertigen als in den Vereinigten Staaten. So darf in Deutschland explizite Preisgabe zur Sicherung der Selbstbestimmung verhindert werden (durch Unterstützung informationellen Selbstschutzes und Entscheidungsarchitekturen), nicht aber in den USA.

Weiter kommt den Rechten der Preisgebenden ein unterschiedlicher Stellenwert zu. Wird durch die Preisgabe die informationelle Privatheit Dritter beeinträchtigt, kommt es in Deutschland zu einer gleichberechtigten Abwägung zwischen den Rechten der Preisgebenden und den Rechten der Dritten. In den USA hingegen kommt der Redefreiheit der Preisgebenden ausgesprochen große Bedeutung zu, während die informationelle Privatheit der Dritten nur geringes Gewicht hat. Daher lässt sich die Verhinderung der Preisgabe zum Schutz Dritter in Deutschland leichter rechtfertigen als in den USA.

Schließlich besitzen die Rechte der verantwortlichen Stellen und insbesondere die Berufsfreiheit in Deutschland einen ungleich geringeren Stellenwert als die Redefreiheit der verantwortlichen Stellen in den USA. Daher scheitern dort Entscheidungsarchitekturen zum Schutz abstrakter Allgemeinwohlbelange an der Redefreiheit, während Entscheidungsarchitekturen in Deutschland regelmäßig einen Eingriff in die Berufsfreiheit der verantwortlichen Stellen darstellen, die als Berufsausübungsregel relativ leicht zu rechtfertigen sind. Auch wenn angesichts des sehr hohen Schutzniveaus der Redefreiheit der verantwortlichen Stellen in den Vereinigten Staaten eine Absenkung rechtspolitisch diskutiert wird, zeigt sich dafür derzeit noch keine Mehrheit.

---

[259] Siehe oben Kapitel 3,C.I.

Kapitel 7

Ausblick

Es hat sich gezeigt, dass angesichts vielfältiger Gefahren für die Preisgebenden sowie für die Allgemeinheit in beiden Rechtsordnungen ein rechtspolitisches Bedürfnis nach Verhinderung informationeller Preisgabe bestehen kann. Dieses bedarf der Umsetzung in verfassungskonformer Weise. So verlockend es zunächst scheinen mag, die Nutzer um ihrer selbst willen an bestimmter informationeller Preisgabe zu hindern, ist dies in beiden Rechtsordnungen jedoch kein zulässiger Eingriffszweck, solange die Nutzer selbstbestimmt handeln. Um dennoch ein bestmögliches Schutzniveau zu erreichen, erscheint ein kreativer Ansatz angezeigt.

Im Folgenden wird zunächst untersucht, ob es sinnvoll und rechtlich zulässig ist, die Idee des libertären Paternalismus zur Verhinderung informationeller Preisgabe zum Schutz selbstbestimmt Preisgebender vor sich selbst heranzuziehen (siehe A). Im Anschluss wird der alternative Ansatz des partiellen informationellen Selbstschutzes entwickelt (siehe B) und ein Ausblick auf gemeinsame Forschungsmöglichkeiten gegeben (siehe C).

A. Libertärer Paternalismus als Ausweg?

Der Schutz der selbstbestimmten Nutzer vor sich selbst stellt de lege lata in Deutschland und in den Vereinigten Staaten gerade keinen zulässigen Rechtfertigungsgrund zur Verhinderung informationeller Preisgabe dar. Fast schon populär ist es aber derzeit insbesondere[1] in den USA, zur Verhinderung informationeller Preisgabe die Idee des libertären Paternalismus als Instrument fruchtbar zu machen, mit Hilfe dessen die Verhinderung informationeller Preisgabe hinsichtlich der Nutzerrechte keine verfassungsrechtliche Rechtfertigung erfordern könnte. Ausgehend vom Leitbild des homo economicus schlagen gewichtige Stimmen vor, die Nutzer durch die Anwendung libertär paternalistischer Maßnahmen zur Beschränkung ihrer informationellen Preisgabe auf das Maß zu bewegen, das ihren rationalen Interessen entspricht.[2] Solche Maßnahmen werden nicht als Eingriff in die Nutzerrechte gese-

---

[1] Auch die deutsche Bundesregierung zeigt jüngst Interesse an dieser Form der Bürgerbeeinflussung, siehe *Hoffmann*, Politik per Psychotrick, 11.3.2015.

[2] Siehe beispielsweise: *Acquisti/Grossklags*, What Can Behavioral Economics Teach us about Privacy?, in: Acquisti/Gritzalis/Lambrinoudakis u. a. (Hrsg.), Digital privacy, 2008, 363 ff.; *Acquisti*, Nudging Privacy, 6 IEEE Security & Privacy Economics (2009), 82 ff.; *Solove*, Privacy

hen, sondern als Mittel, um diesen Rechten Geltung zu verschaffen. Eine Rechtfertigung hinsichtlich der Belange der Nutzer (nicht jedoch hinsichtlich der Rechte der verantwortlichen Stellen) wäre damit entbehrlich.

Zurückgehend auf *Feinberg* ist die Rede vom autonomie-orientierten, weichen Paternalismus.[3] Andere Ausformungen und Begriffe sind der liberale Paternalismus,[4] der sanfte Paternalismus,[5] „behaviour change policies“,[6] der Anti-Antipaternalismus[7] oder der neue Paternalismus.[8]

Hinter den aufgezählten Schlagwörtern verbirgt sich eine Bandbreite verschiedener paternalistischer Interventionen, die sich der Maßnahmen bedienen, die im Rahmen dieser Arbeit als Mittel der Entscheidungsarchitektur bezeichnet werden.[9] Während eine hergebrachte Anwendung der Verfassungsdogmatik sowohl in Deutschland als auch in den Vereinigten Staaten dazu führt, dass diese Mittel als Eingriff in die Nutzerrechte der verfassungsrechtlichen Rechtfertigung bedürfen,[10] könnte die Einordnung als libertär-paternalistische, den Nutzern dienende Maßnahmen eine abweichende Beurteilung erlauben.

Die Mittel sind dadurch gekennzeichnet, dass das Selbstbestimmungsrecht der Betroffenen jedenfalls als Orientierungspunkt gilt. Selbstschädigende Entscheidungen werden nicht, wie im Falle des sogenannten harten Paternalismus, wegen ihres Inhaltes korrigiert, sondern nur dann, wenn jedenfalls die hinreichende Vermutung besteht, sie seien fehlerhaft zustande gekommen.[11] Der Unterschied zwischen weichem und hartem Paternalismus wird dahingehend beschrieben, dass nur ersterer autonome Entscheidungen kompetenter Personen grundsätzlich respektiert und sich bei der Ausgestaltung von Selbstverfügungsschranken am Ziel der Autonomiegewährleistung der Betroffenen orientiert.[12] Weicher Paternalismus beein-

---

Self-Management and the Consent Dilemma, 126 Harvard L. Rev. (2013), 1880 ff. und *Wang/Leon/Chen u. a.*, From Facebook Regrets to Facebook Privacy Nudges, 74 Ohio State L. J. (2013), 1307 ff.

[3] *Feinberg*, Legal Paternalism, in: Sartorius (Hrsg.), Paternalism, 1983, 3, 17; siehe auch: *Fateh-Moghadam*, Grenzen des weichen Paternalismus, in: Fateh-Moghadam/Sellmaier/Vossenkuhl (Hrsg.), Grenzen des Paternalismus, 2010, 21, 26; *Gutwald*, Autonomie, Rationalität und Perfektionismus, in: Fateh-Moghadam/Sellmaier/Vossenkuhl (Hrsg.), Grenzen des Paternalismus, 2010, 73, 74 und *Kirste*, Harter und weicher Rechtspaternalismus, JZ 2011, 805 ff.

[4] *Eidenmüller*, Liberaler Paternalismus, JZ 2011, 814 ff.

[5] *Isensee*, Privatautonomie, in: Isensee/Kirchhof (Hrsg.), Handbuch des Staatsrechts der Bundesrepublik Deutschland VII, 2009, 207 ff., Rn. 33.

[6] *Jones/Pykett/Whitehead*, Governing temptation, 35 Progress in Human Geography (2011), 483.

[7] *Jolls/Sunstein/Thaler*, A Behavioral Approach to Law and Economics, 50 Stanford L. Rev. Online (1998), 1471, 1541 ff.

[8] *Rizzo/Whitman*, Little Brother is Watching You, 51 Arizona L. Rev. (2009), 685.

[9] Siehe oben Kapitel 4,C.

[10] Siehe oben Kapitel 6,A.I.1 und Kapitel 6,B.I.1.

[11] *Mayr*, Grenzen des weichen Paternalismus II, in: Fateh-Moghadam/Sellmaier/Vossenkuhl (Hrsg.), Grenzen des Paternalismus, 2010, 48, 61.

[12] *Fateh-Moghadam*, Grenzen des weichen Paternalismus, in: Fateh-Moghadam/Sellmaier/Vossenkuhl (Hrsg.), Grenzen des Paternalismus, 2010, 21, 27.

flusst Verhalten indirekt, wohingegen harter Paternalismus nur durch Zwang wirkt.[13]

Aus den verschiedenen sich ähnelnden Begründungsansätzen und Formen des Paternalismus durch Entscheidungsarchitekturen soll im Folgenden der am weitesten entwickelte und derzeit einflussreichste herausgegriffen werden: der im Rahmen der insbesondere in den Vereinigten Staaten durchgeführten verhaltensökonomischen Analyse des Rechts entwickelte libertäre Paternalismus.

Zunächst wird die Prämisse des rationalen Handels aller Marktteilnehmer dargelegt (siehe I) und aufgezeigt, warum es zu einem Versagen des Privatheitsmarktes kommt (siehe II). Auf dieser Grundlage wird erläutert, dass informationelle Preisgabe häufig stattfindet, obwohl dies aus rationaler Sicht nicht zu erwarten gewesen wäre (siehe III). Vertreter des libertären Paternalismus erklären dies damit, dass Nutzer unter vorhersehbaren Rationalitätsdefiziten leiden (siehe IV), die der Korrektur bedürften (siehe V).

Dieses Argumentationsmuster wird einer eigenen Bewertung unterzogen (siehe VI), die voraussichtliche Rechtsentwicklung in den Vereinigten Staaten diskutiert (siehe VII) und die Frage nach der Übertragbarkeit des Konzepts auf Deutschland beantwortet (siehe VIII).

I. Prämisse des rationalen Handelns aller Marktteilnehmer

Die Beobachtung, informationelle Privatheit werde zu einem Wirtschafts- oder Tauschgut,[14] zeigt, dass informationeller Privatheit ein Wert zugemessen wird, sodass die Nutzer sie gegen andere Güter eintauschen können.

Um die Aushandlung des individuellen Wertes von Privatheit nachvollziehen zu können, wird die Ökonomische Analyse des Rechts bemüht (im Englischen diskutiert unter den Schlagwörtern Economic Analysis of Law oder Law and Economics). Diese untersucht, welchen impliziten Preis eine rechtliche Regel einem Verhalten auferlegt, wie sich Modifizierungen der Regel auf den impliziten Preis und das menschliche Verhalten auswirken würden und ob diese Auswirkungen aus Effizienzgesichtspunkten wünschenswert sind.[15] Sanktionen wirken dabei wie Preise; auf schwerwiegendere negative Sanktionen reagieren die Akteure durch Einschränkung der sanktionierten Aktivitäten.[16] Ausgangspunkt ist die Mikroökonomie als

---

[13] *Douglas*, Cooperative Paternalism versus Conflictful Paternalism, in: Sartorius (Hrsg.), Paternalism, 1983, 171, 173.

[14] *Rössler*, Der Wert des Privaten, 2001, 218, 232 und *Weichert*, Die Ökonomisierung des Rechts auf informationelle Selbstbestimmung, NJW 2001, 1463 ff.

[15] *Cooter/Ulen*, Law & Economics, 62010, 4. Eine kritische Rezeption liefert: *Lüdemann*, Die Grenzen des homo oeconomicus und die Rechtswissenschaft, in: Engel/Englerth/Lüdemann u. a. (Hrsg.), Recht und Verhalten, 2007, 7 ff. Maßgebliche Prägung erfuhr die deutsche Ökonomische Analyse des Rechts durch: *Eidenmüller*, Effizienz als Rechtsprinzip, 1995, 17 ff.

[16] *Cooter/Ulen*, Law & Economics, 62010, 3.

Untersuchung der Frage, wie begrenzte Ressourcen effizient auf sich ausschließende Ziele verteilt werden können.[17]

Da alle Akteure, so die ökonomische Grundannahme, stets rational handeln (Rational-Choice-Theorie), streben sie danach, irgendetwas zu maximieren, seien es auch nicht-monetäre Güter wie ihre Zufriedenheit oder die Bewahrung ihrer Privatheit.[18] Sie sind rational eigennützig. Als rational Handelnde kennen sie ihre Präferenzen und können alle Alternativen danach einstufen, wie sehr sie ihren Bedürfnissen entsprechen. Die Vorlieben sind dabei subjektiv.[19] Rationalität ist nicht gleichzusetzen mit objektiver Vernünftigkeit. Vielmehr ist sie gegeben, wenn eine Entscheidung konsequent ist vor dem Hintergrund der gegebenen Überzeugungen und Präferenzen. So kann es beispielsweise rational sein, an Geister zu glauben, solange die Betroffenen stringent von der Existenz von Geistern ausgehen.[20]

Da die Alternativen in der Realität durch Rahmenbedingungen limitiert sind, wählen die rational Handelnden die beste Alternative, die ihnen unter den gegebenen Bedingungen offensteht. Dieser Prozess wird als Maximierung bezeichnet. Das sogenannte Constrained Maximum ist an dem Punkt erreicht, an dem die Grenzkosten dem Grenznutzen entsprechen, also durch eine Erhöhung der Kosten keine verhältnismäßige Erhöhung des Nutzens mehr erzielt werden könnte.[21] Der Prozess bedarf dabei keiner tatsächlichen subjektiven Schlussfolgerung, sondern nur eines Handelns, das sich darstellt, als ob die Handelnden die marginale Nützlichkeit berechnet hätten.[22]

Jedes soziale Phänomen stellt dabei ein Gleichgewicht dar, das durch die Interaktion verschiedener nach Maximierung ihres eigenen Wohls strebender Handelnder entsteht. Dieses besteht, bis es durch äußere Einflussfaktoren gestört wird. In einem perfekten, auf Wettbewerb beruhenden Markt bedarf es daher keinerlei Regulierung.[23]

II. Versagen des Privatheitsmarktes

Zu einem Marktversagen tragen insbesondere vier Phänomene bei, die auch Auswirkungen auf den „Privatheitsmarkt"[24] haben können: Monopole, Externalitäten, öffentliche Güter und Informations-Asymmetrien.[25]

---

[17] *Cooter/Ulen*, Law & Economics, [6]2010, 11 f.

[18] *Cooter/Ulen*, Law & Economics, [6]2010, 12 f. und *Zuiderveen Borgesius*, Consent to Behavioural Targeting in European Law, 7.2013, 22.

[19] *Cooter/Ulen*, Law & Economics, [6]2010, 19.

[20] *Kahneman*, Thinking, Fast and Slow, 2011, 411.

[21] *Cooter/Ulen*, Law & Economics, [6]2010, 22.

[22] *Cooter/Ulen*, Law & Economics, [6]2010, 469.

[23] *Cooter/Ulen*, Law & Economics, [6]2010, 294.

[24] *Schwartz*, Property, Privacy, and Personal Data, 117 Harvard L. Rev. (2004), 2055, 2076 ff.

[25] Zu den folgenden Ausführungen, soweit nicht anders angegeben: *Cooter/Ulen*, Law & Economics, [6]2010, 38 ff.

Monopole können dazu führen, dass der zu zahlende Preis für ein Gut mangels Wettbewerbs über den Grenzkosten der Herstellung liegt. Dies kann verhindert werden, indem entweder die Monopole durch Wettbewerb ersetzt werden oder der durch den Monopolisten verlangte Preis reguliert wird.

Weiter kann das fehlende Einfließen von Kosten, die nicht die Parteien, sondern Dritte oder die Allgemeinheit treffen (Externalitäten), zu Marktversagen führen. Um ein solches zu verhindern, müssen die externen Kosten internalisiert werden, sie also den Parteien insoweit auferlegt werden, dass diese im Ergebnis nicht entsprechend ihren privaten Grenzkosten, sondern den sozialen Grenzkosten (also unter Berücksichtigung der Kosten, die die Allgemeinheit treffen) agieren.[26] Damit lässt sich auch begründen, dass informationelle Preisgabe durch die Rechte Dritter und gesellschaftliche Belange limitiert werden darf und hinsichtlich der Belange Dritter in Deutschland sogar muss.

Drittens können die Besonderheiten von öffentlichen Gütern wie nationaler Sicherheit oder sauberer Luft zu Marktversagen führen. Öffentliche Güter sind zunächst dadurch gekennzeichnet, dass sie nicht in Rivalität konsumiert werden, der Konsum durch eine Person also nicht die durch eine andere Person konsumierbare Menge verringert. Weiter besteht kein Ausschlussprinzip bei der Güternutzung: Nicht zahlende Begünstigte können also nicht in wirtschaftlich sinnvoller Weise von der Güternutzung exkludiert werden, sodass im Ergebnis private profitmaximierende Unternehmen nicht zum Angebot des Produkts bereit sind. Um Marktversagen zu verhindern, kann der Staat die Bereitstellung der öffentlichen Güter durch private Unternehmen subventionieren, die Güter selbst zur Verfügung stellen oder (wie im Beispiel des Emmissionszertifikatehandels) durch Regulierung künstliche Märkte schaffen.

Teilweise wird den öffentlichen Gütern auch Privatheit zugerechnet. *Regan* führt in diesem Sinne aus: „the weakness of policy solutions that […] allow one to waive one's privacy rights also would become clear. If one individual or a group of individuals waives privacy rights, the level of privacy for all individuals decreases because the value of privacy decreases."[27] Die von *Regan* nicht ausgesprochene Konsequenz wäre ein staatliches Einschreiten gegen die Preisgabe, um das öffentliche Gut der Privatheit im gesellschaftlichen Interesse zu schützen. *Regan* verknüpft Privatheit bei ihrer zugrunde liegenden Analyse in überzeugender Weise mit drei gesellschaftlichen Werten:[28] Zunächst bestehe ein gemeinsamer Wert („common value"), da alle Individuen irgendeine Form der Privatheit schätzten. Weiter macht sie einen öffentlichen Wert aus („public value"), da Privatheit als Instrument für das Gelin-

---

[26] *Spindler*, IT-Sicherheit, MMR 2008, 7, 8.

[27] *Regan*, Legislating Privacy, 1995, 233.

[28] Zu den folgenden Ausführungen, soweit nichts anderes angegeben: *Regan*, Legislating Privacy, 1995, 213, 220 ff.; daran anknüpfend: *Rössler/Mokrosinska*, Privacy and social interaction, 39 Philosophy and Social Criticism (2013), 772, 773 ff.

gen der Demokratie diene.[29] Schließlich existiere ein kollektiver Wert („collective value“), da es sich bei Privatheit eben um ein öffentliches Gut handele. Individuelle Privatheit könne es nur in Abhängigkeit vom Vorhandensein von Privatheit bei Anderen sowie dem Verhalten der Anderen geben, sie sei unteilbar. Weiter profitierten auch diejenigen, die keinen Beitrag zum Privatheitsschutz leisten, von dem Privatheitsniveau in der Gesellschaft (sogenanntes Trittbrettfahrerproblem). Wie andere öffentliche Güter ließe sich Privatheit also nicht durch den Markt erreichen, vielmehr bedürfe es staatlicher Intervention.

Der Einordnung von informationeller Privatheit als öffentlichem Gut schließt sich auch *Schwartz* an, wenn er von der Existenz von „privacy commons“ spricht. Diese definiert er als „place created through rules for information exchange. It is a multidimensional privacy territory that should be ordered through legislation that structures anonymous and semi-anonymous information spaces.“[30] Informationelle Privatheit lasse sich vergleichen mit sauberer Luft oder Landesverteidigung.[31] Werde informationelle Privatheit nicht gewährleistet, werde die Gesellschaft als Ganze leiden, da Bürger auf eine Reihe zwischenmenschlicher Aktivitäten aus Angst vor der nicht kontrollierbaren Verwendung ihrer personenbezogenen Daten verzichteten.[32]

Schließlich können schwerwiegende Informations-Asymmetrien zu Marktversagen führen. Unterschiedliche Informationslagen sind nichts Außergewöhnliches auf dem Markt und häufig überhaupt erst Grundlage eines Geschäfts. Anderes gilt jedoch, wenn sie so gravierend sind, dass es zu einer Behinderung des Austauschs kommt. Das soziale Optimum kann dann durch den Austausch nicht mehr erreicht werden. Dem kann beispielsweise begegnet werden, indem Verkäufer zur Offenlegung bestimmter für die Käufer nicht ersichtlicher Informationen verpflichtet oder im Privatheits-Kontext den verantwortlichen Stellen Aufklärungspflichten auferlegt werden.

Soweit keine schwerwiegende Informationsasymmetrie vorliegt, kann auch die rechtliche Billigung von durch die Verwender vorgegebenen Einwilligungserklärungen ökonomisch Sinn ergeben:[33] Durch Nutzung unternehmensintern einheitlicher Vorlagen ersparen sich die Verwender hohe Kosten, die durch individuelle Aushandlung und Umsetzung der Bedingungen entstehen würden. Dadurch können die Produkte insgesamt günstiger angeboten werden. Zudem wird, soweit auch konkurrierende Anbieter identische Vorlagen verwenden, die Vergleichbarkeit zwi-

---

[29] Siehe oben Kapitel 3,A.III.3.

[30] *Schwartz*, Property, Privacy, and Personal Data, 117 Harvard L. Rev. (2004), 2055, 2088; vgl. zu einem ähnlichen Ansatz: *Nehf*, Recognizing the Societal Value in Information Privacy, 78 Washington L. Rev. (2003), 1, 61 f.

[31] *Schwartz*, Property, Privacy, and Personal Data, 117 Harvard L. Rev. (2004), 2055, 2084, 2087.

[32] Die Autoren versuchen erkennbar, die unter Kapitel 3,A.III beschrieben Gefahren von Privatheitsverlust für das Allgemeinwohl über neue Wege für die US-amerikanische Privatheits-Diskussion fruchtbar beziehungsweise anschlussfähig zu machen.

[33] *Posner*, Economic Analysis of Law, 72007, 115 ff.

schen den Anbietern erhöht und so der Wettbewerb hinsichtlich des Preises gestärkt.[34] Dabei werden die Bedingungen zwar tendenziell die Verwender besserstellen als die Nutzer. Diese ungleiche Machtverteilung wird jedoch dadurch ausgeglichen, dass die Nutzer, unterstützt beispielsweise durch Medien und Verbraucherschutzorganisationen, bei zu ungünstigen Bedingungen auf andere Anbieter zurückgreifen können. Dieser Aspekt wird verstärkt, indem die Verwender, anders als im Regelfall die Nutzer, einen großen Imageverlust durch einseitige Belastung der Vertragspartner zu befürchten haben. Um dies zu verhindern, werden die rational handelnden Verwender auch das Wohl der Nutzer im Blick haben. Andere Anbieter werden versuchen, durch nutzerfreundlichere Bedingungen einen Wettbewerbsvorteil zu erlangen, sodass der Markt schließlich die für beide Seiten optimalen Bedingungen hervorbringt. Auch bevor ideale Konditionen erreicht sind, werden so jedenfalls unerträgliche Schlechterstellungen verhindert und Verwender sowie Nutzer entlastet, da ihnen der Aushandlungsaufwand erspart bleibt.

III. Preisgabe trotz rational zu erwartender Privatheitswahrung

Grundlage des informationellen Selbstschutzes ist damit aus ökonomischer Sicht die Annahme der stets rational handelnden Nutzer, die aufgrund bereits geformter Präferenzen selbst am besten entscheiden können, was ihnen dient. Preisgabe würde demnach nur dann erfolgen, wenn sie zum Nutzen der Preisgebenden wäre. Dem widersprechen jedoch die Erkenntnisse der Verhaltensökonomie, die feststellt, dass Menschen häufig vorhersehbar irrational handeln. Die verhaltensökonomische Analyse des Rechts versucht, aus dieser Beobachtung Rückschlüsse auf das Recht de lege lata und de lege ferenda zu ziehen.[35]

Wäre den Nutzern nicht an der Bewahrung ihrer Privatheit gelegen, würde die Preisgabe personenbezogener Daten nicht ihren Präferenzen widersprechen. In diese Richtung geht der Ansatz der Post-Privacy-Bewegung.[36] Nach deren Überzeugung wird Privatheit ersetzt durch absolute Transparenz. Dadurch würden wirtschaftliche und politische Macht überprüfbar und wissenschaftlicher Fortschritt

---

[34] *Cooter/Ulen*, Law & Economics, [6]2010, 364.

[35] Eine kritische Einführung liefert: *Englerth*, Behavioral Law and Economics, in: Engel/Englerth/Lüdemann u.a. (Hrsg.), Recht und Verhalten, 2007, 60 ff. Einen Überblick über verhaltensökonomische Untersuchungen informationeller Preisgabe liefern: *Müller/Flender/Peters*, Vertrauensinfrastruktur und Privatheit als ökonomische Fragestellung, in: Buchmann (Hrsg.), Internet Privacy, 2012, 143, 174 ff. *Jolls* analysiert ausführlich, inwieweit US-amerikanische Gerichte bei der Entscheidung über die Gültigkeit erteilter Einwilligungen Aspekte in Betracht ziehen, die auch aus verhaltensökonomischer Perspektive bedeutsam wären: *Jolls*, Rationality and Consent in Privacy Law 2010, 7 ff. Eine Rezeption der Behavioral-Law-and-Economics-Forschung sowie eine Übertragung auf den deutschen Kontext liefert: *van Aaken*, Begrenzte Rationalität und Paternalismusgefahr, in: Anderheiden/Bürkli/Heinig u.a. (Hrsg.), Paternalismus und Recht, 2006, 109 ff. und *dies.*, Das deliberative Element juristischer Verfahren als Instrument zur Überwindung nachteiliger Verhaltensanomalien, in: Engel/Englerth/Lüdemann u.a. (Hrsg.), Recht und Verhalten, 2007, 189, 193 ff.

[36] Zu den folgenden Ausführungen: *Heller*, Post-Privacy, 2011, 137 ff.

vorangetrieben. Sei nichts mehr unbekannt und geheim, steige das Vertrauen, da alle Akteure, Risiken und Möglichkeiten einschätzbar seien. So wäre die Situation für die Gefangenen im Panopticon weit weniger bedrohlich, wenn sie wüssten, wann sie der Blick der Wärter trifft und sie nicht in dauerhafter Angst vor einer möglichen Beobachtung leben müssten. Mit der Zeit pendle sich ein System ein, um den Überfluss an verfügbaren Informationen zu handhaben. Statt einer (Selbst-) Zensur aufseiten der Preisgebenden limitierten die Rezipienten ihre Datenaufnahme auf für sie Relevantes.

Studien zeigen jedoch, dass die Nutzer ihre informationelle Privatheit sehr schätzen und sich durchaus differenzierte Meinungen darüber bilden, welche Daten sie im Austausch gegen welche Gegenleistung preisgeben wollen.[37] Nach einer 2012 in den USA durchgeführten Studie sind bei entsprechender Gegenleistung 81 bis 93 Prozent der Befragten zur Preisgabe von Informationen über ihr Geschlecht und ihren Personenstand bereit, aber nur elf bis 17 Prozent zur Preisgabe ihrer Browser-Historie oder ihrer Mobilfunknummer und nur vier bis sieben Prozent zur Preisgabe ihrer Mobilfunkhistorie oder ihrer E-Mail-Kontakte.[38]

Ähnliche Ergebnisse zeigen sich auch für Deutschland: Nach einer Ende 2010 im Auftrag der Europäischen Kommission durchgeführten Befragung von 26.574 EU-Bürgern lehnen es 62 Prozent der befragten Deutschen (für alle befragten EU-Bürger betrug der Prozentsatz 51 Prozent) absolut ab, personenbezogene Daten im Austausch gegen kostenlose Angebote preiszugeben.[39] 53 Prozent der befragten Deutschen (40 Prozent im EU-Durchschnitt) äußerten sich sehr besorgt über die Aufzeichnung ihres Verhaltens im Internet.[40] Auch nachdem erklärt wurde, dass Online-Anbieter kostenlose Angebote nur anbieten können, wenn sie Werbeeinnahmen erhalten, fühlten sich 24 Prozent der befragten Deutschen sehr unwohl (EU-Durchschnitt: 18 Prozent) und 45 Prozent der befragten Deutschen ziemlich unwohl (EU-Durchschnitt: 36 Prozent) bei dem Gedanken daran, dass ihre personenbezogenen Daten für Targeted Advertising genutzt werden.[41] Nach einer Studie des GfK-Vereins, der 2013 rund 2.000 deutsche Internetnutzer nach ihrem Internetverhalten befragte, lehnen 79 Prozent die Verwendung ihrer im Zusammenhang mit kostenfreien Online-Diensten erhobenen Daten ab.[42]

Es zeigt sich damit eine zurückhaltende Grundhaltung, zu der auch die Datenschutz-Sensibilisierung beitragen dürfte, die in der deutschen und US-amerikanischen Gesellschaft aktuell durch Berichte über Internetüberwachungen diverser Geheimdienste ausgelöst wird.

---

[37] Siehe dazu aktuell: *Trepte/Dienlin/Reinecke*, Privacy, Self-Disclosure, Social Support, and Social Network Site Use, 29.10.2013; Eine Übersicht über ältere Studien bietet: *Nehf*, Shopping for Privacy Online, 1 Univ. of Illinios J. of L., Tech. and Policy (2005), 1, 13 ff.

[38] *Bothun/Lieberman/Tipton*, Consumer privacy, 2012, 4.

[39] *Europäische Kommission*, Special Eurobarometer 359, 6.2011, 33.

[40] *Europäische Kommission*, Special Eurobarometer 359, 6.2011, 68.

[41] *Europäische Kommission*, Special Eurobarometer 359, 6.2011, 75.

[42] *GfK Verein*, Deutsche fürchten Datenmissbrauch, 12.11.2013, 2.

Nutzer scheinen zudem durchaus bereit zu sein, für privatheitswahrende Produkte höhere Preise in Kauf zu nehmen. Eine nicht repräsentative, in den Vereinigten Staaten durchgeführte Studie belegt, dass die Mehrheit der teilnehmenden Nutzer teurere Produkte vorzieht, wenn diese in der Ergebnisliste der Suchmaschine als privatheitswahrend ausgewiesen werden.[43]

Dennoch ergreifen die meisten Nutzer nur in begrenztem Umfang Selbschutzmöglichkeiten. Nach der Studie des GfK-Vereins schalten nur 20 Prozent der Nutzer (27 Prozent der täglichen Nutzer) Cookies in ihrem Brower ab.[44] Nur fünf Prozent (acht Prozent der täglichen Nutzer) verwenden Verschlüsselungsprogramme für E-Mails. Ebenfalls nur fünf Prozent (sechs Prozent der täglichen Nutzer) bedienen sich privatheitswahrender Suchmaschinen wie DuckDuckGo,[45] Disconnect Search[46] oder ixquick[47] – und das, obwohl 61 Prozent personalisierte Suchmaschinenergebnisse ablehnen.[48]

Über ihr eigenes Wohl hinaus können Nutzer zudem ein Interesse an der Vermeidung von Gefahren für Dritte haben, wenn ihnen beispielsweise sonst Unterlassungsansprüche drohen. Zudem kann ein nicht-monetäres, individuelles Interesse an der Vermeidung gesellschaftlicher Nachteile bestehen. Soweit die Nutzer entsprechende Präferenzen haben, kann auch ein der Verwirklichung dieser Interessen abträgliches Verhalten irrational sein.

Da Nutzer häufig trotz der beschriebenen Präferenz zur Privatheitswahrung selbst einfache Schritte zur Erreichung dieses Ziels nicht ergreifen, weicht tatsächliches Verhalten damit nicht selten von rational zu erwartendem ab.[49]

IV. Vorhersehbare Rationalitätsdefizite

Diese Beobachtung wird damit erklärt, dass Nutzer häufig nur mangelhaft informiert sind (siehe 1.) und/oder trotz ausreichender Information die Zusammenhänge kognitiv nicht überblicken können und daher vorhersehbar irrational handeln (siehe 2.).[50]

---

[43] In der Studie analysierte die Suchmaschine auf Basis der P3P-Technologie, inwieweit die Datenschutzrichtlinien der Webseiten mit den Präferenzen der Nutzer übereinstimmten und versah die Suchergebnisse mit entsprechenden Icons: *Tsai/Egelman/Cranor u. a.*, The Effect of Online Privacy Information on Purchasing Behavior, 22 Information Systems Research (2011), 254 ff.

[44] Zu den folgenden Ausführungen, soweit nicht anders angegeben: *GfK Verein*, Maßnahmen der Internetnutzer, 21.11.2013, 2.

[45] Https://duckduckgo.com/.

[46] Https://disconnect.me/search.

[47] Https://www.ixquick.com/.

[48] *GfK Verein*, Deutsche fürchten Datenmissbrauch, 12.11.2013, 2.

[49] *Simitis*, Selbstbestimmung, KJ 1988, 32, 43.

[50] Einen Überblick über verschiedene vorhersehbare Rationalitätsdefizite im Bereich der Preisgabe bieten auch: *Hermstrüwer/Hamann*, Biometrie und Autonomie, in: Hermstrüwer/Hamann/Diers (Hrsg.), Schwimmen mit Fingerabdruck?, 2012, 1, 20 ff.; *dies.*, Biometrie und Behavioral Economics, KJ 2013, 184, 187 ff.

1. Vorhersehbare Informationsdefizite

Auch angesichts ausführlicher Datenschutzerklärungen sind Nutzer häufig nicht ausreichend informiert.[51] Regelmäßig bestehen Informationsasymmetrien, in denen den Nutzern ungleich weniger Fakten über die Folgen der informationellen Preisgabe bekannt sind als den verantwortlichen Stellen.

Hinzu treten kann ein Desinteresse der Nutzer an der Durchdringung der die informationelle Preisgabe betreffenden Fragen. Dies gilt insbesondere für das Lesen und Verstehen vorformulierter Einwilligungserklärungen. Die Verwendung solcher Erklärungen ist an sich wirtschaftlich sinnvoll und kann zu fairen Inhalten führen, wenn jedenfalls eine beachtliche informierte Minderheit die Entscheidung für oder gegen die jeweiligen Anbieter von dem Inhalt der vorformulierten Erklärung abhängig macht und gegebenenfalls auf die Konkurrenz zurückgreift.[52] Wird dem Inhalt jedoch von der ganz überwiegenden Zahl der Einwilligenden keine Beachtung geschenkt, entsteht von Nutzerseite kein Wettbewerb um die Verwendung datenschutzfreundlicher Einwilligungserklärungen und die Nutzer können einseitig belastet werden. Die Probleme vorformulierter Vertragsbedingungen demonstriert beispielsweise eine Studie, die das Browse-Verhalten von 45.091 Haushalten bezüglich 66 Online-Software-Firmen untersuchte. Dabei zeigte sich, dass bei nur 55 von 120.545 Besuchen (0,05 Prozent)[53] auf solchen Webseiten tatsächlich der Lizenzvertrag für mindestens eine Sekunde angeklickt wurde, zudem mit einer Verweildauer von durchschnittlich 47,7 Sekunden nicht lange genug, um die durchschnittlich 2.277 Worte umfassenden Bedingungen lesen zu können.[54] Von 5.509 Besuchen, bei denen sodann eine gesicherte Sitzung hergestellt wurde (wodurch ein tatsächlicher Vertragsschluss indiziert wird), wurden in fünf Fällen (0,11 Prozent) die Vertragsbedingungen aufgerufen.[55] Damit ist davon auszugehen, dass der Inhalt der Vertragsbedingungen beinahe keinen Wettbewerbsvorteil oder -nachteil für die Firmen erzeugte.

Die weitverbreitete Gleichgültigkeit gegenüber dem Inhalt von standardisierten Formularen zeigt auch das Beispiel einer Software Firma, die am 1. April 2010 vorübergehend eine Klausel in ihre Vertragsbedingungen aufnahm, durch die ihr das Recht an der unsterblichen Seele der Käufer übertragen wurde. Die Bestimmung lautete: „By placing an order via this Web site on the first day of the fourth month of the year 2010 Anno Domini, you agree to grant Us a non transferable option to

---

[51] *Rogosch*, Die Einwilligung im Datenschutzrecht, 2013, 78.

[52] Siehe oben Kapitel 7,A.II.

[53] Ein Besuch setzt das Betrachten von mindestens zwei Seiten voraus. Im Durchschnitt wurden 12,4 Seiten während einer Gesamtdauer von 5,2 Minuten betrachtet: *Bakos/Marotta-Wurgler/Trossen*, Does Anyone Read the Fine Print?, Law & Economics Research Paper Series, 10.2009, 26.

[54] *Bakos/Marotta-Wurgler/Trossen*, Does Anyone Read the Fine Print?, Law & Economics Research Paper Series, 10.2009, 1, 3, 26.

[55] *Bakos/Marotta-Wurgler/Trossen*, Does Anyone Read the Fine Print?, Law & Economics Research Paper Series, 10.2009, 27.

claim, for now and for ever more, your immortal soul. Should We wish to exercise this option, you agree to surrender your immortal soul, and any claim you may have on it, within 5 (five) working days of receiving written notification from gamesation.co.uk or one of its duly authorised minions. We reserve the right to serve such notice in 6 (six) foot high letters of fire, however we can accept no liability for any loss or damage caused by such an act. If you a) do not believe you have an immortal soul, b) have already given it to another party, or c) do not wish to grant Us such a license, please click the link below to nullify this sub-clause and proceed with your transaction."[56] Obwohl die optisch hervorgehobene Möglichkeit zum Opt-out bestand und dieser mit einem Fünf-Pfund-Gutschein belohnt wurde, machten nur zwölf Prozent der Käufer von dieser Option Gebrauch. Die übrigen 88 Prozent (ca. 7.500 Käufer) akzeptierten die Klausel.[57]

Die informierte Minderheit ist damit regelmäßig zu klein, um tatsächlichen Einfluss auf die Ausgestaltung der Vertragsbedingungen zu haben.[58] Die entstehende schwerwiegende Informationsasymmetrie zwischen den Preisgebenden und den verantwortlichen Stellen kann aus ökonomischer Sicht zu einem Versagen des Privatheitsmarktes führen.[59]

Die Informationsdefizite erstrecken sich dabei auf das Verständnis für die Gefahren informationeller Preisgabe im Internet und auf Kenntnisse der technischen Abläufe, der möglichen Verwendungsmöglichkeiten, der rechtlichen Rahmenbedingungen sowie der nach der Preisgabe ansetzenden Rechtsbehelfe. Verstärkt wird dieses Phänomen durch die Unsicherheit über die anwendbaren Datenschutzregime, gerade in Bezug auf im Ausland ansässige verantwortliche Stellen.

2. *Vorhersehbar irrationales Verhalten*

Menschen können Informationen nur begrenzt verstehen und verwerten. Gestaltet sich eine Entscheidungsfindung zu kompliziert, kommen vereinfachende, weniger akkurate Strategien zur Anwendung (sogenannte begrenzte Rationalität).[60] Die Komplexität der Folgen informationeller Preisgabe kann dazu führen, dass Nutzer die aus ihr möglicherweise resultierenden Konsequenzen kognitiv nicht oder nur schwer erfassen können.[61] Die Vielzahl verantwortlicher Stellen und die Datenku-

---

[56] Zitiert nach: *Bronwlee*, GameStation EULA collects 7,500 souls from unsuspecting customers, 16.4.2010.

[57] *Bronwlee*, GameStation EULA collects 7,500 souls from unsuspecting customers, 16.4.2010.

[58] *Bakos/Marotta-Wurgler/Trossen*, Does Anyone Read the Fine Print?, Law & Economics Research Paper Series, 10.2009, 28 ff.

[59] Siehe oben Kapitel 7,A.II; *Schwartz*, Property, Privacy, and Personal Data, 117 Harvard L. Rev. (2004), 2055, 2076 ff.

[60] *Nehf*, Shopping for Privacy Online, 1 Univ. of Illinios J. of L., Tech. and Policy (2005), 1, 20 ff.

[61] *Acquisti*, Privacy in Electronic Commerce and the Economics of Immediate Gratification, in: Breese (Hrsg.), Proceedings of the 5th ACM Conference on Electronic Commerce, 2004, 21, 23 f.; *Acquisti/Grossklags*, What Can Behavioral Economics Teach us about Privacy?, in: Acquisti/

mulation bei diesen sind selbst mit Bemühen nicht zu überblicken. So besucht beispielsweise jeder US-Bürger im Durchschnitt monatlich fast einhundert Webseiten, die im Regenfall jeweils wieder Daten an Dritte weitergeben und Datenbestände zusammenführen.[62] Bereits im Jahr 2008 wäre in den USA ein Verdienstausfall von 781 Milliarden Dollar entstanden, wenn alle US-Bürger jeweils alle sie betreffenden Datenschutzerklärungen gelesen hätten; entsprechend mehr, wenn sie zudem Vergleiche zwischen verschiedenen Wettbewerbern angestellt hätten.[63] Die Existenz solcher hohen Transaktionskosten kann aus ökonomischer Sicht wiederum zu Marktversagen führen und ein staatliches Einschreiten notwendig machen.[64]

Mitunter steht auch zum Erhebungszeitpunkt noch gar nicht fest, für welche Zwecke die personenbezogenen Daten später analysiert werden sollen und welche technischen Möglichkeiten sich in der Zukunft bieten werden.[65]

Dazu kommt häufig die Aufbereitung der Fakten in unübersichtlicher Weise in klein gedruckten und sehr langen Einwilligungserklärungen, die durch Wiedergabe einer übermäßigen Fülle an Informationen, von Irrelevantem oder des Gesetzestextes zusätzlich verkompliziert werden.[66] Doch auch die schlichte Auflistung aller relevanten Fakten kann die Nutzer überfordern: Es kommt zum „information overload".[67] Die Rede ist von einem „transparency paradox": Transparenz wird durch detaillierte Aufklärung erzeugt, die Fülle an Informationen führt jedoch zur Unüberschaubarkeit hinsichtlich der relevanten Fakten.[68] Der Grenznutzen zusätzlicher Informationen sinkt oder kann sogar negativ werden.[69]

Durch diese Faktoren bedingt, kann es den Nutzern schwerfallen, alle relevanten Konsequenzen zu erkennen und ihnen die Wahrscheinlichkeiten ihres Eintritts zuzuweisen.[70] Noch pessimistischer äußern sich Stimmen in der Literatur hinsichtlich

---

Gritzalis/Lambrinoudakis u. a. (Hrsg.), Digital privacy, 2008, 363, 364 und *Nehf*, Recognizing the Societal Value in Information Privacy, 78 Washington L. Rev. (2003), 1, 50.

62 *Solove*, Privacy Self-Management and the Consent Dilemma, 126 Harvard L. Rev. (2013), 1880, 1888 f.

63 *McDonald/Faith Cranor*, The Cost of Reading Privacy Policies, 4 I/S: A Journal of Law and Policy for the Information Society (2008), 540, 541.

64 *Zuiderveen Borgesius*, Consent to Behavioural Targeting in European Law, 7.2013, 31 ff.

65 *Acquisti/Grossklags*, What Can Behavioral Economics Teach us about Privacy?, in: Acquisti/Gritzalis/Lambrinoudakis u. a. (Hrsg.), Digital privacy, 2008, 363, 367; *Mayer-Schönberger/Cukier*, Big Data, 2013, 153 und *Solove*, Privacy Self-Management and the Consent Dilemma, 126 Harvard L. Rev. (2013), 1880, 1890.

66 *Rogosch*, Die Einwilligung im Datenschutzrecht, 2013, 71 f.

67 *Calo*, Against Notice Skepticism in Privacy (and Elsewhere), 87 Notre Dame L. Rev. (2012), 1027, 1054.

68 *Nissenbaum*, A Contextual Approach to Privacy Online, Daedalus, the Journal of the American Academy of Arts & Sciences 2011, 32, 36.

69 *Eidenmüller*, Liberaler Paternalismus, JZ 2011, 814, 816 m. w. N.

70 *Acquisti/Grossklags*, What Can Behavioral Economics Teach us about Privacy?, in: Acquisti/Gritzalis/Lambrinoudakis u. a. (Hrsg.), Digital privacy, 2008, 363, 369.

der Gefahren der Nutzung sozialer Netzwerke: „there is absolutely no plausible way to assign probabilities to many of the possible outcomes“.[71]

Weiter zeigt sich, dass informationelle Preisgabe auch bei Vorliegen der erforderlichen Informationen und der Fähigkeit zum Verständnis der Zusammenhänge von dem Verhalten abweicht, das bei rationaler Analyse zu erwarten wäre.[72] Eben diese vorhersehbaren Irrationalitäten bieten den Ansatzpunkt zum Einsatz der beschriebenen Entscheidungsarchitekturen.[73]

V. Defizitkorrektur

Ohne staatliches Eingreifen käme es daher zu einem Versagen des Privatheitsmarktes. Die Erkenntnis, dass Nutzer vorhersehbar irrational ihre informationelle Privatheit preisgeben, wird zum Anlass genommen, die auftretenden Irrationalitäten zu korrigieren.

Plakativ macht dies die Aussage der Vorreiter des libertären Paternalismus *Sunstein* und *Thaler* deutlich: „The presumption that individual choices should be respected is usually based on the claim that people do an excellent job of making choices, or at least that they do a far better job than third parties could possibly do.“[74] Lediglich in einer Fußnote weisen sie daraufhin, dass Grund für die Ablehnung von Paternalismus auch der Vorrang der individuellen Autonomie sein könnte, selbst wenn dadurch Entscheidungsfehler gemacht werden. Dieses Argument schränken sie jedoch sogleich ein: „We do not disagree with the view that autonomy has claims of its own, but we believe that it would be fanatical […] to treat autonomy, in the form of freedom of choice, as a kind of trump not to be overridden on consequentialist grounds.“[75]

Dieser Denklogik folgend, wären individuelle Entscheidungen nur dann zu respektieren, wenn sie rational sind. Sind sie es nicht, wird vorgeschlagen, auf die Entscheidung einzuwirken, um tatsächliches Verhalten und aus rationaler Perspektive wünschenswertes anzugleichen.[76] Dabei wurden traditionell die Fehler in der Entscheidungsfindung hingenommen und lediglich die Ergebnisse korrigiert. Um diese eingriffsintensiven Fälle des harten Paternalismus zu limitieren, werden derzeit verstärkt Maßnahmen vorgeschlagen, die direkt die Fehler in der Entscheidungsfin-

---

[71] *Grimmelmann*, Saving Facebook, 94 Iowa L. Rev. (2009), 1137, 1160.

[72] *Volkmann*, Darf der Staat seine Bürger erziehen?, 2012, 43 ff.

[73] Siehe oben Kapitel 4,C.

[74] *Sunstein/Thaler*, Libertarian Paternalism is Not an Oxymoron, 70 Chicago L. Rev. (2003), 1159, 1167 und *dies.*, Libertarian Paternalism, 93 AEA Papers and Proceedings (2003), 175, 176.

[75] *Sunstein/Thaler*, Libertarian Paternalism is Not an Oxymoron, 70 Chicago L. Rev. (2003), 1159, 1167, Fn. 22.

[76] Zum Beispiel der Zigarettensteuer: „imperfect rationality still provides a basis for paternalism.“: *Lucas, JR.*, Saving Smokers From Themselves, 80 Univ. of Cincinnati L. Rev. (2012), 693, 718; zu Warnhinweisen auf Zigarettenschachteln: *Baehr*, A New Wave of Paternalistic Tobacco Regulation, 95 Iowa L. Rev. (2010), 1663, 1671 f.

dung verhindern oder jedenfalls verringern sollen (Debiasing through Law).[77] Ein Beispiel hierfür ist die rechtliche Anordnung libertär paternalistischer Maßnahmen. Solche Maßnahmen sind insofern paternalistisch, als der Staat für die Bürger entscheidet, wie sie sich am besten zu verhalten haben. Die Bürger werden auch hier Objekte staatlicher Entscheidungen, die fehlerhaft, missbräuchlich oder durch lobbyistische Einflussnahme geprägt sein können. So bewegte beispielsweise Facebook 2012 den U.S. Congress zu einer Gesetzesänderung, die es ermöglichte, eine Liste der über das Video-Stream-Portal Netflix gesehenen Filme zu teilen. „They found it more efficient to nudge Congress than their millions of users."[78] Zugleich seien die vorgeschlagenen Maßnahmen jedoch libertär, da es den Bürgern letztendlich frei stehe, sich trotz gegenteiliger Anreize so zu verhalten, wie sie möchten.[79] Der Staat wird zum „Entscheidungsarchitekten", zugleich steht die Entscheidungsfreiheit der Einzelnen im Fokus.[80] Wenn eine Differenzierung zwischen hartem und weichem Paternalismus nur mit der Begründung gänzlich abgelehnt wird,[81] beide Formen erfolgten gegen den Willen der Betroffenen, wird dabei verkannt, dass einmal gegenteiliges Verhalten der Betroffenen verhindert wird, während es im anderen Fall möglich bleibt. Entscheidungsarchitekturen böten sich nach Ansicht ihrer Befürworter immer dann an, wenn die zu fällenden Entscheidungen schwierig und selten zu treffen sind, die Individuen nicht umgehend Rückmeldung bekommen oder sie nicht alle Aspekte problemlos verstehen können.[82]

Dabei wird teilweise keine strikte Grenze zwischen Unterrichtungsvorschriften und libertär paternalistischen Maßnahmen gezogen.[83] Dem ist zuzugestehen, dass es das Wesen der Unterrichtung ist, beispielsweise Über-Optimismus[84] durch verstärkte Faktenkenntnis abzubauen. Jedoch können an beide unterschiedliche Rechtfertigungsanforderungen zu stellen sein, wie sich beispielsweise in den USA an der Entscheidung R.J. Reynolds Tobacco Co. v. Food and Drug Admin.[85] zeigt, nach der erzwungene normative kommerzielle Rede (und damit Entscheidungsarchitektur) schwieriger zu rechtfertigen ist als erzwungene unkontroverse kommerzielle Rede

---

[77] *Jolls*, Rationality and Consent in Privacy Law 2010, 65 ff.; generell zur Idee des Debiasing: *Fischhoff*, Debiasing, in: Kahneman/Slovic/Tversky (Hrsg.), Judgement under uncertainty, 1982, 422 ff.

[78] *Calo*, Code, Nudge, or Notice?, 4.2013, 13.

[79] *Sunstein*, The Storrs Lectures, 122 Yale L.J. (2013), 1826, 1835.

[80] *Thaler/Sunstein*, Nudge, ²2012, 11, 14.

[81] So *Kirste*, Harter und weicher Rechtspaternalismus, JZ 2011, 805, 808.

[82] *Thaler/Sunstein*, Nudge, ²2012, 106 ff.

[83] Beispielsweise bei: *Jolls*, Rationality and Consent in Privacy Law, 2010, 65 ff.; *Acquisti* betont jedenfalls den Unterschied zwischen der Verbesserung der Benutzbarkeit, die die Umsetzung einer Entscheidung erleichtert und libertärem Paternalismus, der das Treffen einer Entscheidung beeinflusst: *Acquisti*, Nudging Privacy, 6 IEEE Security & Privacy Economics (2009), 82, 84.

[84] Dazu: *Oskamp*, Overconfidence in case-study judgments, in: Kahneman/Slovic/Tversky (Hrsg.), Judgement under uncertainty, 1982, 287 ff.

[85] R.J. Reynolds Tobacco Co. v. Food and Drug Admin., 696 F.3d 1205 (D.C. Cir. 2012); siehe oben Kapitel 6,B.I.2.

(und damit eine Unterrichtungsvorschrift zur Unterstützung informationellen Selbstschutzes). Aufgrund der unterschiedlichen rechtlichen Konsequenzen bedarf es daher einer Differenzierung nach Maßnahmen, die die Nutzer nur neutral informieren möchten (Unterrichtung) und solchen, die sie in eine bestimmte Richtung lenken wollen (libertär paternalistisch).

Zudem ist der Übergang zwischen libertär paternalistischen Maßnahmen und einem erzwungenen Schutz fließend.[86] So kann ein strafbewehrtes gesetzliches Verbot als ein Zwang gewertet werden, jedoch auch als ein Anreiz, die Handlung zu unterlassen. Zur Abgrenzung erscheint es sinnvoll, als libertär paternalistisch einzustufen, was den Nutzern keine oder nur eine geringe Belastung auferlegt und sie zugleich in eine Richtung lenken soll.

Im Kontext der informationellen Preisgabe böten sich nach Ansicht der Befürworter des libertären Paternalismus die dargestellten Maßnahmen der Entscheidungsarchitektur an,[87] jedoch nur, soweit sie den rationalen Interessen der Individuen Geltung verschaffen sollen. Dann werden sie als rechtmäßig angesehen, ohne dass nach einem entsprechenden Eingriffstitel hinsichtlich der Rechte der Preisgebenden gefragt würde.

VI. Bewertung

Das Umgehen der Rechtfertigungsbedürftigkeit eines Eingriffs in die Rechte der Preisgebenden durch Anwendung libertär paternalistischer Maßnahmen erscheint fragwürdig.[88] Die Erkenntnis, dass die allermeisten Menschen nur beschränkt rational sind, rechtfertigt an sich noch gar nichts, auch keine staatlichen Eingriffe.[89] Kenntnisse über Verhaltensanomalien dürfen daher nicht als paternalistische Ad-hoc-Rechtfertigungen für staatliche Interventionen missbraucht werden.[90] Dieser Ansicht schließt sich jüngst auch der ehemalige Verfassungsrichter *Di Fabio* an, wenn er darauf verweist, dass „die moderne Gesellschaft, die zunehmend einen öffentlichen Tugendkodex vorschreibt“, akzeptieren müsse, „dass unsere Grundrechte die Minderheitenrechte der Eigenwilligen sind“.[91]

---

[86] Zum fließenden Übergang und der Berechtigung beider Kategorien: *Sunstein*, The Storrs Lectures, 122 Yale L. J. (2013), 1826, 1858 ff.

[87] Siehe oben Kapitel 4,C.

[88] Zu dieser Kritik auch: *Sandfuchs/Kapsner*, Coercing Online Privacy, 11 I/S: A Journal of Law and Policy for the Information Society (2016), (im Erscheinen); vgl. *dies.*, Nudging as a Threat to Privacy, 6 Rev. of Philosophy and Psychology (2015), 455 ff.

[89] *Van Aaken*, Begrenzte Rationalität und Paternalismusgefahr, in: Anderheiden/Bürkli/Heinig u. a. (Hrsg.), Paternalismus und Recht, 2006, 109, 110, 135.

[90] *Van Aaken*, Begrenzte Rationalität und Paternalismusgefahr, in: Anderheiden/Bürkli/Heinig u. a. (Hrsg.), Paternalismus und Recht, 2006, 109, 110.

[91] *Der Spiegel*, „Wir sind keine Labormäuse“, Der Spiegel 15/2015, 38, 39. Angesichts aktueller Pläne der Bundesregierung, verstärkt auf den Einsatz von Entscheidungsstrukturen zur Lenkung der Bürger zu setzen, verweist er zudem darauf, dass in den entsprechenden Situationen Verbote zum Schutz der Bürger vor sich selbst nicht gerechtfertigt wären, sodass auch Entscheidungsarchitekturen unzulässig sein dürften. Ebenso verweist er jedoch darauf, dass eine Rechtfertigung der

Während sich in der deutschsprachigen Literatur auch einige kritische Stimmen finden,[92] wird der Argumentationsansatz in den Vereinigten Staaten überwiegend hingenommen. Vereinzelt wird angemerkt, dass die verhaltensökonomische Analyse des Rechts das jüngste Einfallstor in die Paternalismus-Debatte darstellt.[93] Doch auch diese Kritik stützt sich nicht etwa darauf, dass der Schutz selbstbestimmt Handelnder vor sich selbst prinzipiell unzulässig sei. Vielmehr wird darauf hingewiesen, dass erstens nicht jeder Mensch vorhersehbar irrational handelt und zweitens das Forschungsgebiet der Verhaltensökonomie noch zu jung ist, um verlässliche Aussagen treffen zu können.[94] Diese Einwände sind zwar richtig, verfehlen aber das grundlegende Problem, dass auch irrationales Handeln selbstbestimmtes Handeln darstellt.

Es wird eine Notwendigkeit erkannt, in bestimmten Situationen Maßnahmen zu treffen, um selbstbestimmt Handelnde vor sich selbst zu schützen. Da dies jedoch den Grundfesten einer liberalen Verfassungstradition zuwiderliefe, wird ein anderer Begründungsansatz herangezogen. Unter Verweis auf Erkenntnisse der Verhaltensökonomie werden libertär paternalistische Maßnahmen gefordert. Diese sollen den Individuen gerade zur Wahrnehmung ihrer Rechte verhelfen und sie nicht etwa bevormunden.

Dabei wird übersehen, dass trotz guter Absichten Entscheidungen der Individuen beeinflusst werden. Der Verweis auf libertär paternalistische Maßnahmen wird so unmerklich zur Eingriffsrechtfertigung. Libertär paternalistische Maßnahmen beginnen, die traditionelle, liberale Begrenzung staatlicher Befugnisse zu umgehen und eröffnen so neue Möglichkeiten für legitimes staatliches Einschreiten.[95] Diese Maßnahmen stehen gerade in den Vereinigten Staaten im Zusammenhang mit dem Willen, die staatliche Intervention in das Alltagsleben zu rechtfertigen. Es liegt in

---

Entscheidungsarchitekturen aus Allgemeinwohlgründen (z. B. zum Schutz der Umwelt) möglich sein kann, *dies.*, „Wir sind keine Labormäuse“, Der Spiegel 15/2015, 38 f. Den Ausführungen ist uneingeschränkt zuzustimmen.

[92] *Van Aaken*, Begrenzte Rationalität und Paternalismusgefahr, in: Anderheiden/Bürkli/Heinig u. a. (Hrsg.), Paternalismus und Recht, 2006, 109 ff.; *Englerth*, Vom Wert des Rauchens und der Rückkehr der Idioten, in: Engel/Englerth/Lüdemann u. a. (Hrsg.), Recht und Verhalten, 2007, 231, 235 f.; *Gutwald*, Autonomie, Rationalität und Perfektionismus, in: Fateh-Moghadam/Sellmaier/Vossenkuhl (Hrsg.), Grenzen des Paternalismus, 2010, 73 ff.; *Joost*, Begrenzte Rationalität und ärztliche Aufklärungspflichten, in: Fateh-Moghadam/Sellmaier/Vossenkuhl (Hrsg.), Grenzen des Paternalismus, 2010, 126, 150 f. Nach *Eidenmüller* ist rechtlicher Paternalismus dann legitim, wenn er freiheitsfördernde Effekte mit sich bringt: *Eidenmüller*, Effizienz als Rechtsprinzip, 1995, 375.

[93] *Camerer/Issacharoff/Loewenstein u. a.*, Regulation for Conservatives, 151 Univ. of Pennsylvania L. Rev. (2003), 1211, 1214.

[94] *Camerer/Issacharoff/Loewenstein u. a.*, Regulation for Conservatives, 151 Univ. of Pennsylvania L. Rev. (2003), 1211, 1214.

[95] *Jones/Pykett/Whitehead*, Governing temptation, 35 Progress in Human Geography (2011), 483, 483, 486 (aus britischer Perspektive).

Wahrheit ein klassischer Fall des Paternalismus vor – der Staat entscheidet, was für die Nutzer am besten ist.[96]

Die Autonomie der Einzelnen gewährleistet ihnen, ihre eigenen Entscheidungen zu fällen, auch wenn diese nachteilig sind oder später bereut werden. Nicht jede objektiv nachteilige Entscheidung stellt eine irrationale Entscheidung dar[97] und es ist nicht zwingend rational, zukünftiges Wohlergehen kurzfristigen Vorteilen vorzuziehen.[98] Doch selbst wenn eine Entscheidung irrational ist, ist sie im Regelfall selbstbestimmt – nur eben nicht im besten Interesse der Nutzer.

Die Beobachtung, dass Nutzer irrationale Entscheidungen fällen, ist richtig. Doch der Schluss, dass diese korrigiert werden müssen, geht fehl. Vielmehr werden der Anlass zum Einsatz von Entscheidungsarchitekturen und ihre Rechtfertigung unzulässigerweise gleichgesetzt. Warum jedoch Grund für staatliches Einschreiten bestehen soll, wenn die Nutzer irrationale, aber selbstbestimmte Entscheidungen treffen, ist zweifelhaft: Es erscheint nicht offensichtlich, weshalb erstens eine durch nicht rationale Faktoren beeinflusste Entscheidung nachteiliger sein sollte als eine unbeeinflusste[99] und warum zweitens der Staat aufgerufen sein sollte, diese Entscheidung zu korrigieren.

Richtigerweise muss vielmehr die Autonomie der Nutzer im Vordergrund stehen. Es bleibt möglich, den Nutzern ihr Wohlergehen aufzuzwingen, jedoch nur in den aufgezeigten verfassungsrechtlichen Grenzen. Keinesfalls dürfen libertär paternalistische Maßnahmen als Einfallstor für Bevormundung dienen.[100]

Hinzu tritt ein zweites Argument, das entschieden gegen libertär paternalistische Argumentationsmuster spricht: Sollen die Nutzer von außen dazu bewegt werden, das Ziel zu erreichen, welches ihren Präferenzen entspricht, müssen ihre Ziele bekannt sein. Solange Entscheidungsarchitekten keine Gedanken lesen können, müssen sie, beispielsweise basierend auf Datenanalyse, versuchen, die internen Präferenzen der Nutzer möglichst genau zu bestimmen.[101] Da Rationalität keiner Verobjektivierung zugänglich ist, werden die Entscheidungsarchitekten bei der Bestimmung der vermeintlichen Nutzerpräferenzen ihre eigenen Vorstellungen der Wirklichkeit und ihre Werte zugrunde legen und damit die Nutzervorstellungen

---

[96] *Mitchell*, Libertarian Paternalism Is an Oxymoron, 5.2002 FSU College of Law, Law and Economics Paper, 1, 12, Fn. 37.

[97] *Mitchell* nennt das Beispiel des rationalen Sadisten oder Masochisten: *Mitchell*, Libertarian Paternalism Is an Oxymoron, 5.2002 FSU College of Law, Law and Economics Paper, 1, 28.

[98] *Hill*, Anti-Anti-Anti Paternalism, 2 New York J. of L. and Liberty (2007), 444, 445 f.

[99] Zweifelhaft erscheint im Übrigen, ob es so etwas wie eine „unbeeinflusste Entscheidung“ überhaupt gibt, da auch der Einsatz von Entscheidungsarchitektur wiederum zur Beeinflussung führen würde.

[100] Ausführlich: *Rizzo/Whitman*, Little Brother is Watching You, 51 Arizona L. Rev. (2009), 685 ff.

[101] Dieser Vorschlag wird ausgiebig erörtert bei: *Porat/Strahilevitz*, Personalizing Default Rules and Disclosure with Big Data, 112 Mich. L. Rev. (2014), 1417 ff.

übergehen. Diese Art der Bevormundung ist inhärent in libertär-paternalistischen Maßnahmen, aber kaum mit der Vorstellung einer selbstbestimmten Entscheidungsfindung der Betroffenen vereinbar.

Außerhalb des Privatheits-Kontextes werden zudem vereinzelt sogar Beispiele angeführt, in denen Entscheidungsarchitekturen zu einer Verhaltensbeeinflussung genutzt werden, die nicht den rationalen Interessen der Individuen dient. Beispielhaft für eine solche „libertarian benevolence“ sind Standardvorgaben, nach denen Arbeitnehmer einen Teil ihres Einkommens automatisch an gemeinnützige Zwecke spenden.[102] Damit wird implizit zugestanden, dass Entscheidungsarchitekturen genutzt werden können, um staatliche Zwecke durchzusetzen. Das Argument, es sei im rationalen Interesse der Spendenden, einen Teil ihres Einkommens wegzugeben, lässt sich schwerlich anführen. Vielmehr setzt der Staat seine Ziele durch. Soweit diese legitim sind und die eingesetzten Maßnahmen weniger restriktiv als andere, darf er dies auch. Aber es bedarf richtigerweise entsprechender Prüfung.

VII. Rechtsentwicklung in den USA

Trotz der hier geäußerten Skepsis erscheint die Rechtsentwicklung in den Vereinigten Staaten offen. Entscheidungsarchitekturen sind nicht am Ersten Zusatzartikel der Preisgebenden, sondern lediglich am prozessualen Due-Process-Standard zu messen.[103] Ausreichend ist somit, dass die Maßnahme in einem nachvollziehbaren Verhältnis zu einem legitimen Zweck steht, wobei die Beweislast bei den Betroffenen liegt. Es erscheint möglich, dass Gerichte die hier vorgetragenen Bedenken nicht teilen und einen Verstoß gegen prozessualen Due Process ablehnen werden.

Dabei könnte eine Rolle spielen, dass Entscheidungsarchitekturen jedenfalls den Central-Hudson-Test hinsichtlich der gemäß dem Ersten Zusatzartikel geschützten Rechte der verantwortlichen Stellen bestehen müssen[104] und somit eine verfassungsrechtliche Überprüfung möglich ist. Der Test schreibt strenge Standards vor und geht bei Weitem über die Rechtfertigungsanforderungen hinaus, die zur Einhaltung von prozessualem Due Process beachtet werden müssen. Soweit verantwortliche Stellen dazu verpflichtet werden sollen, normative Rede wiederzugeben, also solche, die eine staatliche Wertung enthält, sind die Maßnahmen nur gerechtfertigt, wenn ein substanzieller staatlicher Zweck verfolgt wird, die Maßnahme direkt den Zweck fördert und sie nicht umfangreicher als erforderlich ist. Diesen Beweis zu erbringen, kann im Einzelfall eine hohe Hürde darstellen. Gerichten würde daher weniger Begründungsaufwand abverlangt, wenn sie die Entscheidungsarchitekturen als unvereinbar mit den Rechten der verantwortlichen Stellen erklären würden,

---

[102] *Sunstein/Thaler*, Libertarian Paternalism is Not an Oxymoron, 70 Chicago L. Rev. (2003), 1159, 1185.

[103] Siehe oben Kapitel 6,B.I.1.a)bb).

[104] Siehe oben Kapitel 6,B.I.2.c).

als wenn sie den Beweis erbringen müssten, dass ein Verstoß gegen den prozessualen Due Process-Standard hinsichtlich der Rechte der Preisgebenden vorliegt.

VIII. Übertragung auf Deutschland

Zu Beginn des Kapitels schien es, als könnte es wünschenswert für den deutschen Staat sein, mithilfe libertär paternalistischer Argumente eine Verhinderung selbstbestimmter informationeller Preisgabe zu erreichen. Entscheidungsarchitekturen sind in tatsächlicher Hinsicht auch in Deutschland anwendbar. Doch die verfassungsrechtlichen Bedenken, die gegen den Schutz selbstbestimmt Preisgebender sprechen, namentlich der Vorrang autonomer Entscheidungsfindung vor staatlicher Bevormundung,[105] behalten ihre volle Gültigkeit. Das Argument, durch libertären Paternalismus würde Selbstbestimmung nicht etwa genommen, sondern ermöglicht, überzeugt nicht.

Bereits die Analyse des US-Verfassungsrechts zeigt die schwache Grundlage, auf die sich die weitgehend unhinterfragte Heranziehung libertär paternalistischer Argumente zum Schutz selbstbestimmt Handelnder vor sich selbst stützt. Eine Übertragung dieses Ansatzes auf Deutschland erscheint, jedenfalls soweit es um den verbindlichen Einsatz von Entscheidungsarchitekturen zum Schutz selbstbestimmt Preisgebender vor sich selbst geht, nicht zielführend und damit – um auf die Ausgangsfrage dieses Kapitels zurückzukommen – kein sachgerechter Ausweg.

Davon unabhängig können verantwortliche Stellen jedoch freiwillig Entscheidungsarchitekturen einsetzen, um die Nutzer bei der Preisgabe in dem Maße zu unterstützen, das deren Interessen entspricht. Unter Umständen kann dieses Vorgehen von den Nutzern dankbar angenommen werden und einen Marktvorteil für die verantwortlichen Stellen erzeugen.

B. Partieller informationeller Selbstschutz

Sowohl in Deutschland als auch in den Vereinigten Staaten kann ein rechtspolitisches Bedürfnis bestehen, informationelle Preisgabe in bestimmten Fällen zu verhindern. Dieses bedarf der Umsetzung in verfassungskonformer Weise.

Die schnell fortschreitende technische Entwicklung ist nicht zeitgleich rechtlich zu fassen. Vielmehr werden in Wissenschaft und Praxis verschiedenartige Modelle diskutiert, die einen Beitrag zum Schutz vor den Gefahren informationeller Preisgabe leisten können. Das folgende Kapitel will die bestehenden Ansätze systematisieren und speziell auf die Verhinderung informationeller Preisgabe anwenden.

---

[105] Siehe oben Kapitel 6,A.I.1.c).; siehe auch die aktuelle zutreffende Analyse durch den ehemaligen Verfassungsrichter *Di Fabio*: *Der Spiegel*, „Wir sind keine Labormäuse“, Der Spiegel 15/2015, 38 ff.

Wie sich gezeigt hat, sind Freiheitsbeschränkungen mit dem alleinigen Zweck, die selbstbestimmt Preisgebenden vor sich selbst zu schützen, in beiden Rechtsordnungen verfassungswidrig. Daran ändert sich auch nichts, wenn die staatliche Intervention darauf abzielt, selbstbestimmte, aber irrationale Preisgabe zu verhindern. Dennoch ist ein Schutz der Preisgebenden vor sich selbst in verfassungskonformer Weise erzielbar – nicht pauschal, sondern gerade in den Situationen, in denen das größte Gefahrenpotenzial besteht: Wird staatlicherseits festgestellt, dass bestimmte informationelle Preisgabe so gewichtige Nachteile für die Preisgebenden oder die Allgemeinheit mit sich bringt, dass ihre Verhinderung rechtspolitisch wünschenswert erscheint, kann in drei Schritten vorgegangen werden. Dieser Ansatz des partiellen informationellen Selbstschutzes besitzt Überzeugungskraft sowohl für das deutsche als auch für das US-amerikanische Rechtssystem.

Zur Verhinderung informationeller Preisgabe bieten sich in dieser Reihenfolge an:

- die Verhinderung nicht selbstbestimmter informationeller Preisgabe (siehe I),
- die Verhinderung informationeller Preisgabe, die Allgemeinwohlbelange gefährdet (siehe II) sowie schließlich
- die Unterstützung informationellen Selbstschutzes (siehe III).

I. *Verhinderung nicht selbstbestimmter Preisgabe*

Zunächst kann nicht selbstbestimmte informationelle Preisgabe verhindert werden. Derartige Maßnahmen können in beiden Rechtsordnungen gerechtfertigt werden, in Deutschland besteht sogar eine entsprechende Schutzpflicht.

Angesichts des fließenden Übergangs zwischen selbstbestimmten und nicht selbstbestimmten Entscheidungen erscheint ein staatliches Tätigwerden bereits angezeigt in „Konstellationen, die zumindest den bösen Schein erwecken, dass es sich nicht wirklich um eine autonome Entscheidung handelt und heteronome Motive nicht ausgeschlossen werden können“.[106] Dabei wäre es mit der Sicherheit und Leichtigkeit des Rechtsverkehrs unvereinbar, vor jeder informationellen Preisgabe individuell festzustellen, ob die jeweiligen Nutzer tatsächlich über Einsichtsfähigkeit und Wahlmöglichkeit verfügen.[107] Ein solches System würde zu erheblicher Rechtsunsicherheit führen, wäre wirtschaftlich sinnlos und offenkundig nicht praktikabel.

Beiden Staaten steht es daher frei, unter Wahrung des Gleichbehandlungsgrundsatzes zu typisieren. Dieser wird durch Art. 3 Abs. 1 GG beziehungsweise die Due-Process-Klauseln gewährleistetet. In Abgrenzung zu einer bloßen Generalisierung oder Pauschalisierung liegt eine Typisierung vor, wenn eine Gesetzesformulierung Besonderheiten des Einzelfalls außer Acht lässt, die jedoch nach dem Norm-

[106] *Fisahn*, Ein unveräußerliches Grundrecht am eigenen genetischen Code, ZRP 2001, 49, 54 (wenn auch im Kontext der Veräußerung des genetischen Codes).

[107] Vgl. zu § 104 BGB: Beck-OK BGB/*Wendtland*, 2015, § 104, Rn. 2.

zweck relevant gewesen wären.[108] Sie ist mit dem allgemeinen Gleichbehandlungsgrundsatz vereinbar, wenn ihr Zweck, regelmäßig also die Verhinderung einer übermäßig komplizierten Rechtssetzung und -anwendung, gewichtig genug ist, um die Ungleichbehandlung zu rechtfertigen.[109]

Der Staat darf unter diesen Umständen im Rahmen der Typisierung beispielsweise Altersgrenzen festsetzen, vor deren Erreichen von fehlender und nach deren Erreichen von bestehender Einsichtsfähigkeit ausgegangen wird (vergleichbar den Typisierungen in §§ 104 ff. BGB und Sec. 1302 f. Children's Online Privacy Protection Act[110]). Ebenso darf er in bestimmten Situationen typisiert von fehlender Wahlmöglichkeit ausgehen, soweit die Kategorisierungen nachvollziehbar sind. Dass dabei im Einzelfall beispielsweise besonders „reife" Minderjährige oder besonders willensstarke objektiv benachteiligte Preisgebende als nicht selbstbestimmt behandelt werden, ist der notwendige Preis für ein praktikables Rechtssystem. Gelingt allerdings keine nachvollziehbare Typisierung, liegt ein Verstoß gegen die Grundrechte der Betroffenen vor.

Ein Ansatzpunkt für eine zulässige Typisierung kann das Konzept des asymmetrischen Paternalismus sein. Ein solcher soll vorliegen, wenn eine Regelung denjenigen, die sonst Fehler begehen würden, große Vorteile bringt, aber gleichzeitig diejenigen, die vollständig rational handeln, nur geringfügig belastet.[111] Richtigerweise ist jedoch nicht auf die Rationalität der Handelnden, sondern auf deren Selbstbestimmtheit abzustellen. Es kann daher gelten: Im Rahmen des asymmetrischen Paternalismus ist die typisierte Verhinderung einer Preisgabe regelmäßig sachgerecht, wenn diese denjenigen, die sonst nicht selbstbestimmt handeln, große Vorteile bringt (also vor schwerwiegenden Gefahren schützt, die durch nicht selbstbestimmte Preisgabe entstanden wären), aber diejenigen, die selbstbestimmt handeln, nur geringfügig belastet (etwa, weil kein herausragendes Interesse an der Preisgabe bestand oder weil vergleichbare Formen der Preisgabe möglich bleiben).

Durch eine großzügige Handhabung der Typisierung wird auch verhindert, dass Nutzer durch faktische Zwänge zur Preisgabe veranlasst werden. Solange keine selbstbestimmte Preisgabe möglich ist, läuft auch der Verweis auf die Eigenverantwortung der Nutzer ins Leere.

Ergänzt wird der Schutz nicht selbstbestimmt Preisgebender in Deutschland durch eine an den Staat adressierte Pflicht, Maßnahmen zur Sicherung der Selbstbestimmung zu ergreifen.[112] Zulässig sind hierzu sowohl die Unterstützung informationellen Selbstschutzes als auch Entscheidungsarchitekturen. Zwar dürfen Letztere

---

[108] *Britz*, Einzelfallgerechtigkeit versus Generalisierung, 2008, 38.

[109] *Britz*, Einzelfallgerechtigkeit versus Generalisierung, 2008, 40.

[110] 15 U.S.C. § 6501 ff., umgesetzt durch die Children Online Privacy Protection Rule, 16 C.F.R. § 312.

[111] *Camerer/Issacharoff/Loewenstein u. a.*, Regulation for Conservatives, 151 Univ. of Pennsylvania L. Rev. (2003), 1211, 1212.

[112] Siehe oben Kapitel 5,A.V.3.

nur angewandt werden, wenn die Unterstützung informationellen Selbstschutzes nicht effektiv genug ist. Man wird jedoch zugestehen müssen, dass viele Nutzer kognitiv, technisch und auch zeitlich mit der Aufgabe überfordert sind, auf sich allein gestellt über alle mit der Preisgabe zusammenhängenden Fragen zu entscheiden.[113] Bisweilen wird Selbstschutz daher gar als „unrealistische Perspektive“[114] bezeichnet – schon für entsprechend vorgebildete Akteure in Wissenschaft und Politik, erst recht für das Gros der Bevölkerung. Auch aus ökonomischer Sicht liegt es nicht im Interesse der Gesellschaft, dass Nutzer einen signifikanten Teil ihrer kognitiven und zeitlichen Ressourcen auf ständig neu anfallende Entscheidungen über Privatheitsaufgaben verwenden.

Die Effektivität der reinen Unterstützung des Selbstschutzes lässt sich damit häufig ablehnen und es scheint sinnvoll, in Deutschland in Standardsituationen ergänzend auf den verpflichtenden Einsatz privatheitsschützender Voreinstellungen zurückzugreifen. Dadurch bleibt den Nutzern Zeit, sich auf die Entscheidung spezieller Preisgabefragen zu konzentrieren. Solange der Einsatz von Entscheidungsarchitekturen der Sicherung der Selbstbestimmung dient, ist er verfassungsrechtlich rechtfertigbar und kann auch in deutlich weiterem Umfang als bislang angewandt werden.

Während in Deutschland eine Pflicht besteht, zur Sicherung der Selbstbestimmung sowohl explizite (also bewusste und zielgerichtete) als auch implizite (also technisch im Hintergrund erfolgende, häufig unbewusste) Preisgabe zu verhindern, darf in den USA lediglich impliziter Preisgabe entgegnet werden. Dabei können in Deutschland Entscheidungsarchitekturen angewandt werden, wenn die Unterstützung informationellen Selbstschutzes nicht wirksam genug ist. Dies wird häufig der Fall sein. In den USA sind Entscheidungsarchitekturen an sich auch immer dann zulässig, wenn die Unterstützung informationellen Selbstschutzes nicht wirksam genug ist. Hierbei wird jedoch ein strengerer Prüfungsmaßstab angelegt als in Deutschland, wie die Entscheidung U.S. West, Inc. v. FCC belegt, in der die Zulässigkeit von Opt-in-Regelungen zur Datenerhebung verneint wurde: „[T]he FCC record does not adequately show that an opt-out strategy would not sufficiently protect customer privacy. The respondents merely speculate that there are a substantial number of individuals who feel strongly about their privacy, yet would not bother to opt-out if given notice and the opportunity to do so. Such speculation hardly reflects the careful calculation of costs and benefits that our commercial speech jurisprudence requires.“[115] Auch wenn entsprechend die Sicherung von Selbstbestimmung

---

[113] Diese Einschätzung scheint in der Literatur geteilt zu werden, statt vieler: *Kutscha*, Erster Teil, in: Kutscha/Thomé (Hrsg.), Grundrechtsschutz im Internet?, 2013, 11, 44 ff.; zu den Konsequenzen des sogenannten Digital Divide für den staatlichen Schutzauftrag: *Heckmann*, Öffentliche Privatheit, K&R 2010, 770, 774.

[114] *Hoffmann-Riem*, Freiheitsschutz in den globalen Kommunikationsinfrastrukturen, JZ 2014, 53, 54.

[115] U.S. West, Inc. v. FCC, 182 F.3d 1224, 1239 (10th Cir. 1999); siehe Kapitel 6,B.I.2.

in den Vereinigten Staaten derzeit weitgehend durch Unterstützung informationellen Selbstschutzes erfolgt, werden in der US-amerikanischen Literatur Veränderungen angemahnt: „[M]any people do not want to micromanage their privacy. They want to know that someone is looking out for their privacy and that they will be protected from harmful uses.“[116]

Auf lange Sicht gesehen erscheint es daher sachgerecht und – für Deutschland und möglicherweise auch für die Vereinigten Staaten – realistisch, dass den Bürgern um der Sicherung ihrer Selbstbestimmung willen die Last genommen wird, jede Privatheitsfrage eigenverantwortlich entscheiden zu müssen, sie mithin also von der Verantwortung befreit werden, „to micromanage their privacy“.

II. Verhinderung von Preisgabe, die Allgemeinwohlbelange gefährdet

Zweiter Ansatzpunkt ist die Verhinderung informationeller Preisgabe, die Allgemeinwohlbelange gefährdet, also entweder die Rechte Dritter oder gesellschaftliche Belange wie kulturelle Entwicklung und die Demokratie.[117]

1. Spielraum bei der Bestimmung des primären Schutzzwecks

Wie sich gezeigt hat, wirken sich die durch informationelle Preisgabe entstehenden Gefahren in zwei Richtungen aus: in Richtung der Preisgebenden selbst sowie in Richtung des Allgemeinwohls. Entsprechend kann die Verhinderung informationeller Preisgabe entweder den Schutz der Preisgebenden oder den Schutz des Allgemeinwohls bezwecken. Wird der Schutz der Preisgebenden beabsichtigt, liegt eine paternalistische Intervention vor. Darunter ist jedes Handeln zu verstehen, das zum Wohle der Betroffenen auch ohne oder gegen deren Willen erfolgt.[118] Ansonsten liegt eine Maßnahme zum Schutz des Allgemeinwohls vor.

Doch ein näherer Blick offenbart eine unscharfe Trennlinie zwischen beiden Schutzzwecken. Selbstschädigendes Verhalten hat regelmäßig jedenfalls mittelbare Auswirkungen auf Andere, sei es auch nur dadurch, dass bei diesen Unwohlsein oder Mitgefühl ausgelöst wird oder – außerhalb des hiesigen Kontexts – den Sozialkassen Kosten auferlegt werden.

Nach *Mill* sind „alle Einzelheiten des persönlichen Lebens und Treibens“ privat, die nur die Individuen selbst betreffen „oder wenn sie andere auch betreffen, sodann mit ihrer freien, unabhängigen und nicht durch Täuschung erlangten Zustimmung

---

[116] *Solove*, Privacy Self-Management and the Consent Dilemma, 126 Harvard L. Rev. (2013), 1880, 1901.

[117] Siehe oben Kapitel 3,A.III.

[118] *Eidenmüller*, Liberaler Paternalismus, JZ 2011, 814, 815; *Fateh-Moghadam*, Grenzen des weichen Paternalismus, in: Fateh-Moghadam/Sellmaier/Vossenkuhl (Hrsg.), Grenzen des Paternalismus, 2010, 21, 22. Grundlegenden Einblick in philosophische und rechtspolitische Paternalismus-Konzepte gibt der Sammelband: *Sartorius* (Hrsg.), Paternalism 1983; zum Begriff des „legal paternalism“ als Anwendung des Paternalismus durch den Gesetzgeber: *Feinberg*, Legal Paternalism, in: Sartorius (Hrsg.), Paternalism, 1983, 3 ff.

und Teilnahme."[119] Er konzediert, dass eine selbstschädigende Handlung nicht mehr nur die Einzelnen betreffe, wenn sie die Sympathien wie auch die Interessen der ihnen Nahestehenden ernstlich in Mitleidenschaft zieht.[120] Diesen Befund schränkt er jedoch sogleich ein, wenn er annimmt, selbstschädigendes Verhalten tangiere nur die Einzelnen, solange diese weder eine besonders geartete Pflicht gegen die Öffentlichkeit verletzen noch nachweislich einem Anderen außer sich selbst ersichtlichen Schaden zufügen.[121]

Auch *Dworkin* gesteht zu, dass es nicht einfach ist, Beispiele für rein paternalistisch motivierte Interventionen zu finden.[122] Er zählt jedoch eine Reihe jedenfalls signifikant paternalistisch angetriebener Maßnahmen auf, unter anderem:

- Verpflichtungen zum Tragen von Motorradhelmen,
- Verbot, an öffentlichen Stränden zu schwimmen, wenn kein Rettungsschwimmer anwesend ist,
- Suizidverbot,
- Verbot gegenüber Frauen und Kindern, in bestimmten Berufen zu arbeiten,
- Einschränkungen einvernehmlicher sexueller Praktiken zwischen Erwachsenen,
- Verbot des Drogenkonsums, solange er nicht zu anti-sozialem Verhalten führt,
- verpflichtende Sozialversicherungsbeiträge,
- Glücksspielverbot,
- Beschränkungen von Darlehenszinsen,
- Verbot des Duellierens,
- Verbot, sich zu versklaven,
- Verbot der Tötung auf Verlangen sowie
- Flouridzusätze im Trinkwasser.[123]

Bezeichnend ist jedoch, dass *Dworkin* diese Beispiele keineswegs als rein paternalistische Maßnahmen, sondern lediglich als signifikant paternalistisch getriebene Interventionen einordnet. Mit etwas Kreativität lassen sich jeweils auch Allgemeinwohlbelange ausmachen, die als Motivation für die staatliche Intervention dienen könnten. Es ist somit kaum ein selbstgefährdendes Verhalten denkbar, das nicht jedenfalls mittelbar auch Auswirkungen auf die Allgemeinheit hat.

Um die Interessen und Verhaltensweisen der Einzelnen jedoch nicht vollständig dem Wohl der Allgemeinheit unterzuordnen, erscheint es sinnvoll, eine Grenze zwischen beiden Schutzzwecken zu ziehen. Auch wenn diese keineswegs starr ist, kann sie einen Anhaltspunkt für die rechtliche Einordnung geben. Als Richtschnur erscheint es sachgerecht, zu unterscheiden zwischen solchen Maßnahmen, die primär die jeweiligen Individuen schützen (paternalistische Schutzrichtung) und sol-

[119] *Mill*, Über die Freiheit, 2010 (Original: 1859), 22.
[120] *Mill*, Über die Freiheit, 2010 (Original: 1859), 117.
[121] *Mill*, Über die Freiheit, 2010 (Original: 1859), 118.
[122] *Dworkin*, Paternalism, in: Sartorius (Hrsg.), Paternalism, 1983, 19, 20.
[123] *Dworkin*, Paternalism, in: Sartorius (Hrsg.), Paternalism, 1983, 19, 20.

chen, die jedenfalls auch in signifikanter Weise deren Umwelt zugutekommen sollen (Schutz von Allgemeinwohlbelangen).

Die Bestimmung der primären Schutzrichtung ist dem Staat überlassen. In den beiden Rechtsordnungen zeigen sich jedoch Unterschiede darin, wie weit die Einschätzungsprärogative des jeweiligen Gesetzgebers reicht.

In Deutschland steht dem Gesetzgeber bei der Beurteilung der Eignung und Erforderlichkeit des gewählten Mittels sowie bei der Einschätzung und Prognose der den Einzelnen oder der Allgemeinheit drohenden Gefahren ein Beurteilungsspielraum zu, der vom Bundesverfassungsgericht je nach der Eigenart des in Rede stehenden Sachbereichs, der Möglichkeiten, sich ein hinreichend sicheres Urteil zu bilden und der auf dem Spiel stehenden Rechtsgüter nur in begrenztem Umfang überprüft werden kann.[124] In den USA hingegen ist die Einschätzungsprärogative deutlich geringer als in Deutschland.[125] Berührt eine Maßnahme den Schutzbereich eines verfassungsmäßigen Rechts in einer Weise, dass sie nur nach den strengsten Anforderungen (der sogenannten Strict Scrutiny) gerechtfertigt werden kann, schließt dies eine Eingriffsrechtfertigung häufig aus, ohne dass Spielraum für eine Güterabwägung bestünde. Wenn in den USA beispielsweise eine Maßnahme nicht nur Zeit und Ort einer Meinungsäußerung regelt, sondern deren Inhalt betrifft, kann dieser Eingriff in die Redefreiheit ausschließlich dann gerechtfertigt werden, wenn ein zwingender staatlicher Zweck verfolgt wird, der nicht auch durch weniger restriktive Mittel gleich wirksam erreicht werden kann.[126] Diese hohe Hürde wird nur in seltenen Fällen überwunden.

Soweit der verfassungsrechtliche Spielraum jeweils reicht, ist es zur Erreichung eines effektiven Schutzes vor den Gefahren informationeller Preisgabe zulässig, von den Einschätzungsprärogativen großzügigen Gebrauch zu machen.[127] Ein solches Vorgehen geht keineswegs über das verfassungsrechtlich Zulässige hinaus, sondern findet zahlreiche Vorbilder in der bisherigen Rechtsprechungspraxis in beiden Staaten. Wie anhand der folgenden Beispiele demonstriert wird, gehen Gerichte in anderen Konstellationen auch bereits jetzt nicht allzu zögerlich bei der Verhinderung selbstgefährdenden Verhaltens vor, das gleichzeitig (wenn auch nicht sehr naheliegende) Allgemeinwohlgefährdungen mit sich bringt. Der Schutz der sich selbst gefährdenden Grundrechtsträger ist in diesen Fällen zulässiger Nebeneffekt. Die Konstellation lässt sich treffend als „gemischter Paternalismus“ charakterisieren.[128]

---

[124] St. Rspr., statt vieler: BVerfGE 90, 145 (173).

[125] *Lange*, Grundrechtsbindung des Gesetzgebers, 2010, 219 ff. m. w. N.

[126] Die Idee der Strict Scrutiny geht zurück auf: United States v. Carolene Products Co., 304 U.S. 144, 152, Fn. 4 (1938).

[127] In diese Richtung geht auch *Allen*: „Thus, there will be a legitimate basis for mandating privacy and duties of privacy that do not involve paternalism – a simple application of Mill’s harm principle.“ Im Unterschied zu hier lässt sie jedoch darüber hinaus auch rein paternalistische Maßnahmen zu, *Allen*, Our Privacy Rights and Responsibilities, 13 Philosophy and Law (2013), 19, 23.

[128] *Heinig*, Paternalismus im Sozialstaat, in: Anderheiden/Bürkli/Heinig u. a. (Hrsg.), Paternalismus und Recht, 2006, 157, 175.

2. Rechtsprechung in Deutschland

Ist ein staatliches Einschreiten zum Schutz der Rechte Dritter geboten, kann dies als zulässigen notwendigen Nebeneffekt den Schutz der Einzelnen vor selbstgefährdender Freiheitsausübung mit sich bringen. Die Rechtsprechung hält Beispiele bereit, in denen der nach den Ausführungen der Gerichte primär bezweckte Schutz Dritter zudem in signifikanter Weise zum Schutz der Schädiger vor sich selbst führt:

Die Anschnallpflicht für Autofahrer dient nach Ansicht des Bundesverfassungsgerichts dem Schutz anderer Verkehrsteilnehmer, da Unfallbeteiligte, die durch den Schutz des Sicherheitsgurtes nicht oder nur leicht verletzt worden sind, eher noch sachgerecht reagieren können, um die Schädigung anderer Verkehrsteilnehmer zu vermeiden. Der Sicherheitsgurt kann zudem dagegen schützen, dass bei einer Kollision Fahrzeuginsassen gegen andere geschleudert werden.[129] Mit dieser Argumentation umgeht das Bundesverfassungsgericht die eigentlich bestehende Notwendigkeit, zu begründen, dass der Sache nach die Gesundheit der Insassen gegen ihren Willen geschützt wird.

Ähnlich dient eine Helmpflicht für Motorradfahrer nach Ansicht des Bundesverfassungsgerichts auch der Gesellschaft, da Unfälle mit schweren Kopfverletzungen diese belasten, beispielsweise durch den Einsatz der Rettungsdienste, durch ärztliche Versorgung, durch Rehabilitationsmaßnahmen und durch die Versorgung von Invaliden.[130] Damit wird offenkundig als Nebenzweck auch die Gesundheit der Motorradfahrer selbst geschützt. Die an sich hier geteilte Argumentation des Bundesverfassungsgerichts ist jedoch insofern abzulehnen, als ersparte Sozialkosten zur Rechtfertigung herangezogen werden. Die Anerkennung finanzieller Aspekte als Gemeinwohlbelang öffnet Missbrauch in Gestalt eines inflationären Einsatzes paternalistischer Regelungen Tür und Tor.[131]

Wie das Bundesverfassungsgericht weiter entschied, bezweckt das Betäubungsmittelrecht die Gestaltung des sozialen Zusammenlebens in einer Weise, die es von sozialschädlichen Wirkungen des Umgangs mit Drogen freihält, da insbesondere die Festigung der Persönlichkeit von Jugendlichen und Heranwachsenden durch

---

[129] BVerfG NJW 1987, 180, 180; siehe zur Problematik schon früh: *Münch*, Grundrechtsschutz gegen sich selbst?, in: Stödter/Thieme (Hrsg.), Festschrift für Hans Peter Ipsen zum siebzigsten Geburtstag, 1977, 113, 115 ff.

[130] BVerfGE 59, 275 (279); zur Problematik: *Münch*, Grundrechtsschutz gegen sich selbst?, in: Stödter/Thieme (Hrsg.), Festschrift für Hans Peter Ipsen zum siebzigsten Geburtstag, 1977, 113, 115 ff.; ablehnend: *Lisken*, Freispruch für „Gurtmuffel“, NJW 1985, 3053 ff. Anders als für Motorradfahrer besteht für Fahrradfahrer keine Helmpflicht. Wie der Bundesgerichtshof 2014 entschied, ist Fahrradfahrern das Nicht-Tragen eines Helms jedenfalls innerorts bei einem Unfall auch nicht als anspruchskürzendes Mitverschulden anzulasten: BGH NJW 2014, 2493.

[131] Zurecht kritisch: *Dietlein*, Die Lehre von den grundrechtlichen Schutzpflichten, 1992, 229; *Doehring*, Die Gesunderhaltung des Menschen im Spannungsverhältnis zwischen Staatsfürsorge und Individualentscheidung, in: Fürst/Herzog/Umbach (Hrsg.), Festschrift für Wolfgang Zeidler Band II, 1987, 1553, 1557 ff.; für die Anerkennung finanzieller Aspekte als Gemeinwohlbelang: *Schwabe*, Der Schutz des Menschen vor sich selbst, JZ 1998, 66, 72 ff.

Rauschmittelgenuss behindert werden kann.[132] Impliziter Nebeneffekt ist auch hier der Schutz der Konsumenten vor den Folgen der Drogeneinnahme.

Auch das Verbot des sogenannten Zwergenweitwurfs stellt nach dem Urteil des Verwaltungsgerichts Neustadt neben dem umstrittenen aufgedrängten Menschenwürdeschutz jedenfalls auch auf die Rechte Dritter ab, da durch das Werfen von Menschen das beachtliche Risiko des Abbaus von Hemmschwellen im Umgang mit anderen Menschen besteht.[133]

Selbst in der sogenannten Peep-Show-Entscheidung stützt das Bundesverwaltungsgericht seine Argumentation – neben dem fragwürdigen aufgedrängten Menschenwürdeschutz – auf Gemeinwohlaspekte: Es bezieht sich darauf, dass der Menschenwürde eine über die Einzelnen hinausreichende Bedeutung zukommt.[134]

Den aufgeführten Beispielen ist gemein, dass die in Rede stehenden staatlichen Maßnahmen jedenfalls zu einem beträchtlichen Teil auch den Schutz der sich selbst Gefährdenden bewirken. Auch wenn die zur Rechtfertigung herangezogenen Allgemeinwohlbelange bedeutend sind, zeigt sich doch die Großzügigkeit der Gerichte bei der Entscheidung der Frage, welcher Schutzzweck im Vordergrund steht und welcher Schutz nur als Nebeneffekt eintritt.

Der Schutz von Rechten Dritter oder von gesellschaftlichem Fortschritt und der Demokratie kann damit Hauptzweck von Maßnahmen zur Verhinderung informationeller Preisgabe sein, auch wenn als signifikanter Nebeneffekt selbstbestimmt Preisgebende vor sich selbst geschützt werden. Zu beachten ist dabei, dass der Einsatz dieses gemischten Paternalismus nur zulässig sein kann, wenn sich der Schutz von Allgemeinwohlbelangen in nachvollziehbarer Weise als primärer Zweck darstellen lässt.

3. Rechtsprechung in den USA

Gerichte in den Vereinigten Staaten erkennen ebenfalls Allgemeinwohlbelange als legitimen Zweck zur Rechtfertigung der Verhinderung eines Verhaltens an, auch wenn zugleich als Nebeneffekt die Handelnden vor sich selbst geschützt werden.

Die Beihilfe zum Suizid darf nach Ansicht des U.S. Supreme Court verboten werden unter anderem mit Hinweis auf das staatliche Interesse am Schutz der Integrität des medizinischen Berufs und zur Vermeidung eines zukünftigen Trends zu Euthanasie und anderem Missbrauch.[135] Unausgesprochen wird durch dieses Verbot auch das Leben des Betroffenen geschützt.

Eine Anschnallpflicht für Autofahrer stellt nach Ansicht des Texas Court of Appeals keinen Verstoß gegen die Due-Process-Klausel dar. Das Gericht führt aus: „[T]he Texas seat belt law serves the public safety and welfare by enhancing a dri-

[132] BVerfGE 90, 145 (174).
[133] VG Neustadt NVwZ 1993, 98, 99; siehe oben Kapitel 5,A.V.2.
[134] BVerwGE 64, 274 (280); siehe oben Kapitel 5,A.V.2.
[135] Washington v. Glucksberg, 521 U.S. 702, 728 (1997).

ver's ability to maintain control of his vehicle, and by reducing injuries not only to himself, but also to others, all of which directly affects the state's economic welfare."[136] Der Schutz der Autofahrer vor sich selbst wird also mit der Ersparnis an Gesundheitskosten nach Unfällen sowie mit dem Wohl Dritter gerechtfertigt.

Weiter verstößt eine Helmpflicht für Motorradfahrer nach Ansicht des Texas Court of Criminal Appeals nicht gegen den prozessualen Due-Process-Standard, da das Gesetz dazu dient, das Wohlbefinden und die Sicherheit der Allgemeinheit zu fördern und in einem nachvollziehbaren Zusammenhang zur Sicherheit des Straßenverkehrs generell steht.[137]

Auch der Transfer eigener Organe gegen finanzielle Kompensation ist verboten. Der National Organ Transplant Act verbietet den Transfer von menschlichen Organen gegen vermögenswerte Gegenleistung.[138] Eine vertragliche Verpflichtung zum Transfer eigener Organe ist „clearly repulsive to public policy", der Staat wird daher nicht zu ihrer Durchsetzung tätig.[139] Gleichzeitig wird damit im Nebeneffekt auch die Gesundheit der potenziellen Organverkäufer geschützt.

Auch die Judikatur in den Vereinigten Staaten ist somit großzügig bei der Frage, wann sich selbstgefährdende Tätigkeiten mit Rücksicht auf den Schutz von Allgemeinwohlinteressen verhindern lassen. Eine entsprechend weite Auslegung bietet sich auch bei der Rechtfertigung von Maßnahmen zur Verhinderung informationeller Preisgabe, die Allgemeinwohlbelange gefährdet, an.

III. Unterstützung informationellen Selbstschutzes

Soweit die beiden vorgenannten Rechtfertigungsmöglichkeiten – die Verhinderung nicht selbstbestimmter Preisgabe sowie solcher Preisgabe, die Allgemeinwohlbelange gefährdet – nicht bestehen, bleibt schließlich die Unterstützung informationellen Selbstschutzes. In Ablehnung des libertären Paternalismus wird in diesem Sinne auch ein „liberty-focused paternalis[m]" gefordert, der individuelle Freiheit dem objektiven Wohlergehen vorzieht.[140]

Ergänzend zu den im Verlauf der Arbeit dargestellten Möglichkeiten zur Unterstützung informationellen Selbstschutzes[141] erscheint es vielversprechend, verstärkt mit kartellrechtlichen Instrumenten gegen den Missbrauch marktbeherrschender

---

[136] Richards v. State, 743 S.W.2d 747, 748 (Tex.App.-Hous. 1st Dist. 1987).

[137] Ex parte Smith, 441 S.W.2d 544, 548 (Tex. Crim. App. 1969).

[138] 42 U.S.C. § 274e.

[139] Wilson v. Adkins, 57 Ark. App. 43, 49 (1997).

[140] *Mitchell*, Libertarian Paternalism Is an Oxymoron, 5.2002 FSU College of Law, Law and Economics Paper, 1, 31. Beispiel ist das Subventionieren von Bildung, um den Bürgern Selbstschutz zu ermöglichen: *Klick/Mitchell*, Government Regulation of Irrationality, 90 Minnesota L. Rev. (2006), 1620, 1652.

[141] Diese sind: die konventionelle Unterrichtung, alternative Unterrichtungsmethoden, die Ermöglichung von technischem Selbstschutz und Datenschutz als Bildungsauftrag, siehe oben Kapitel 4,B.

Stellungen durch die verantwortlichen Stellen vorzugehen (siehe 1.).[142] Weiter bietet es sich an, auch in Deutschland mehr Aufmerksamkeit auf das Konzept der regulierten Selbstregulierung und ihre Durchsetzung im Wege des Rechts des unlauteren Wettbewerbs zu legen (siehe 2.) und schließlich eine gestärkte Eigenverantwortung der Nutzer zu akzeptieren und auch einzufordern (siehe 3.).

1. Verhinderung des Missbrauchs marktbeherrschender Stellungen

Informationeller Selbstschutz kann ermöglicht werden, indem den Nutzern eine echte Wahl zwischen Online-Anbietern gewährleistet wird. Häufig besteht ein Machtungleichgewicht zwischen Nutzern und verantwortlichen Stellen bei der Nutzung von Online-Diensten, da es an echten Alternativen fehlt. Dadurch kann in Einzelfällen Druck zur Wahl eines bestimmten Anbieters auf die Nutzer entstehen, auch wenn sie mit dessen Datenschutzrichtlinien nicht einverstanden sind.

Ein möglicher Umgang mit diesem Problem soll am Beispiel sozialer Netzwerke erläutert werden.[143] Diese zeichnen sich dadurch aus, dass die Nutzer innerhalb eines Netzwerks mit anderen Nutzern verknüpft sind, dort unübersehbare Datenstrukturen aufgebaut haben und bislang nur unter Inkaufnahme des Verlusts ihres persönlichen Kontakte-Netzwerks zu einem anderen Anbieter wechseln könnten.

Dem soll durch die LIBE-Fassung des Entwurfs der EU-Datenschutz-Grundverordnung entgegengewirkt werden. Dort ist in Art. 15 Abs. 2a ein Recht auf Datenportabilität enthalten. Den Nutzern würde ein Recht gewährt „to obtain from the controller a copy of the provided personal data in an electronic and interoperable format which is commonly used and allows for further use by the data subject without hindrance from the controller from whom the personal data are withdrawn. Where technically feasible and available, the data shall be transferred directly from controller to controller at the request of the data subject.“ [144] Die Details dieser geplanten Regelung wurden im Laufe der andauernden Diskussion bereits Änderungen unterworfen und es ist noch unklar, ob und wann die Verordnung in Kraft treten

[142] Soweit durch solche Maßnahmen in die Grundrechte der verantwortlichen Stellen, insbesondere in Art. 12 Abs. 1 GG eingegriffen wird, bedarf dies der Rechtfertigung entlang der unter Kapitel 6,A.I.2 dargestellten verfassungsrechtlichen Maßstäbe.

[143] Vgl. zu den folgenden Ausführungen: *Sandfuchs*, Exclusionary Conduct and the Proposed Right to Data Portability, 16.5.2014. Neben der Verhinderung des Missbrauchs marktbeherrschender Stellungen im Bereich der sozialen Netzwerke kann das Kartellrecht noch in weiteren Situationen als Instrument zum Privatheitsschutz der Bürger herangezogen werden: Grundlage für die Prüfung, ob Unternehmensfusionen wettbewerbsrechtlich bedenklich sind, ist die Wahrscheinlichkeit des Markteintritts von Mitbewerbern. Dabei erscheint es sachgerecht, in diese Analyse verstärkt auch den Umstand einzubeziehen, dass große Konzerne wie Google über einen riesigen Datenbestand verfügen, der mögliche Mitbewerber in signifikanter Weise vom Markteintritt abhält, siehe dazu die lesenswerten Ausführungen bei: *Newman*, Search, Antitrust and the Economics of the Control of User Data, 30 Yale J. on Regulation (2014), 401 ff.

[144] Der derzeitige Stand ist abrufbar unter: http://www.janalbrecht.eu/fileadmin/material/Dokumente/DPR-Regulation-inofficial-consolidated-LIBE.pdf.

und ob sie dieses Recht enthalten wird.[145] Zudem wird sich zeigen, wie weitreichend das Recht auf Datenportabilität verstanden werden wird. Bei der Auslegung entscheidend zu berücksichtigen sein werden die Wirtschaftsgrundrechte der Anbieter. Ein Recht auf Datenportabilität greift in diese ein, da den Anbietern zum einen erhebliche Kosten mit der technischen Implementierung auferlegt werden und sie zum anderen gezwungen werden, mehr Wettbewerb zu ermöglichen, wodurch ihre eigenen Umsätze sinken können. Diese Eingriffe lassen sich rechtfertigen mit dem Zweck, den Nutzern den Schutz ihrer Privatheit zu ermöglichen. Jedoch ist das Verhältnismäßigkeitsprinzip zu beachten. Die Angemessenheit kann beispielsweise hergestellt werden, indem der Staat auf eigene Kosten Forschung zur technischen Umsetzbarkeit betreibt und die Datenportabilität auf bestimmte Daten (etwa die eigenen Fotos und Nachrichten) beschränkt. Ob das Recht auf Datenportabiltität dann allerdings noch die erhofften Anreize im Wettbewerb bringt, wird zu klären sein. Würde es dahingehend interpretiert, dass es nur dann anwendbar ist, wenn die technischen Übertragungsmöglichkeiten bereits bestehen („Where technically feasible and available"), wäre der Anwendungsbereich sehr klein und könnte sogar die Entwicklung weiterer Datenübertragungstools behindern. Das Hauptproblem im Zusammenhang mit dem Recht auf Datenübertragbarkeit wird allerdings ein praktisches sein: Die Übertragbarkeit der eigenen Daten allein wird regelmäßig nicht das sein, was die Nutzer wünschen. Vielmehr muss auch gewährleistet sein, dass sie sich weiterhin mit ihren Freunden aus dem ursprünglichen sozialen Netzwerk austauschen können. Dies kann nur durch zusätzliche gesetzliche Vorgaben zur Interoperabilität erreicht werden.[146]

Ergänzend lohnt es sich daher, über einen verstärkten Einsatz kartellrechtlicher Sanktionen nachzudenken, um die Nutzer vor dem Missbrauch marktbeherrschender Stellungen durch Online-Anbieter zu schützen.[147] Ein solches Vorgehen wird unter anderem von *Almunia*, dem bis 2014 amtierenden Wettbewerbskommissar und Vizepräsidenten der Europäischen Kommission, vorgeschlagen.[148] Nach Art. 102 AEUV ist die missbräuchliche Ausnutzung einer marktbeherrschenden Stellung verboten und kann nach Art. 103 AEUV mit Geldbußen und Zwangsgeldern sanktioniert werden. Ein Beispiel für ein solches Vorgehen sind die Maßnahmen der Europäischen Kommission gegen Microsoft: Im vorangegangenen Verfahren[149] hatte sich Microsoft verpflichtet, den Nutzern des Windows Betriebssystems eine Wahlmöglichkeit zwischen dem hauseigenen und alternativen Browsern zur Verfügung zu stellen, um den Vorwurf des Missbrauchs marktbeherrschender Stellungen

---

[145] Die ursprüngliche Fassung fand sich in Art. 18, KOM(2012) 11 final, 25.1.2012.

[146] *Hornung*, Die europäische Datenschutzreform, in: Scholz/Funk (Hrsg.), DGRI Jahrbuch 2012, 2013, 1, 11.

[147] Siehe auch: *Paal*, Vielfaltsicherung im Suchmaschinensektor, ZRP 2015, 34, 35 f.

[148] *Almunia*, Competition and personal data protection, 26.11.2012; befürwortend auch: *Schliesky/Hoffmann/Luch u. a.*, Schutzpflichten und Drittwirkung im Internet, 2014, 161 f.

[149] Europäische Kommission, Entscheidung v. 16.12.2009, C(2009) 10033.

abzuwehren. Das Nichteinhalten dieser Verpflichtung wurde sodann von der Europäischen Kommission 2013 mit einer Geldbuße in Höhe von 561 Millionen Euro sanktioniert.[150]

Erkenntnisse kann auch ein Blick in die Vereinigten Staaten liefern, in denen in den vergangenen Jahren mehrfach versucht wurde, Datenportabilität in sozialen Netzwerken im Wege des Wettbewerbsrechts durchzusetzen. Voraussetzung für einen Wettbewerbsverstoß ist zum einen, dass ein Wettbewerber eine Marktmacht (Market Power) innehat und zum anderen, dass er (potenzielle) Wettbewerber vom Markt ausschließt (Exclusionary Conduct).

Eine Marktmacht kann sich aus dem sogenannten Netzwerk-Effekt ergeben, wenn der Wert des Netzwerks von der Anzahl der in ihm miteinander verbundenen Nutzer abhängt.[151] Erhält ein Produkt allein aufgrund der hohen Anzahl seiner Nutzer einen Wettbewerbsvorteil gegenüber vergleichbaren, jedoch weniger genutzten Produkten, entsteht Marktmacht in diesem Sinne. So hatte beispielsweise das soziale Netzwerk Facebook im Juni 2015 1,31 Milliarden monatliche aktive Nutzer.[152] Nach einer Studie des Pew Research Center aus dem Jahr 2014 haben erwachsene Facebook-Nutzer dort durchschnittlich 338 Kontakte, der Median liegt bei 200.[153] Zwar ließe sich argumentieren, die Nutzer stünden trotz einer großen Anzahl an Kontakten regelmäßig nur im Austausch mit wenigen, sodass ein Netzwerk-Effekt abzulehnen sei.[154] Doch selbst wenn Nutzer nicht mit allen Kontakten gleichermaßen kommunizieren, scheint der Mehrwert sozialer Netzwerke gerade in der Möglichkeit zu liegen, theoretisch mit einer unbegrenzten Anzahl an Menschen in Verbindung treten zu können, die über die Anzahl der bisherigen realen Kontakte hinaus geht. Betreiber von sozialen Netzwerken können daher durchaus über Marktmacht verfügen.

Weiter müsste sich auch ein Ausschluss von Wettbewerbern aus dem Markt nachweisen lassen. Das Fehlen von Datenportabilitäts-Tools spricht für einen Ausschluss von Wettbewerbern. Allerdings hat der D.C. Circuit Court in seiner Grundsatz-Entscheidung United States v. Microsoft zurückhaltend entschieden: „[A] monopolist does not violate the antitrust laws simply by developing a product that is incompatible with those of its rivals. In order to violate the antitrust laws, the incompatible product must have an anticompetitive effect that outweighs any procompetitive justification for the design."[155] Generell statuiert das Wettbewerbsrecht gerade keine Pflicht, mit Wettbewerbern zu kooperieren.[156] Eine derartige Verpflichtung kann nur in sehr speziellen Fällen bestehen, insbesondere, wenn die Verweigerung der

---

150 Europäische Kommission, Entscheidung v. 6.3.2013, C(2013) 1210 final.

151 Dazu ausführlich: *Lemley/McGowan*, Legal Implications of Network Economic Effects, 86 California L. Rev. (1998), 479, 598 ff.

152 Http://www.statisticbrain.com/facebook-statistics/.

153 *Smith*, 6 New Facts About Facebook, 3.2.2014.

154 *Yoo*, When Antitrust Met Facebook, 19 George Mason L. Rev. (2012), 1147, 1151 ff.

155 United States v. Microsoft Corp., 253 F.3d 34, 75 (D.C. Cir. 2001).

156 Verizon Communications Inc. v. Law Offices of Curtis V. Trinko, LLP, 540 U.S. 398 (2004).

Kooperation klar wettbewerbsfeindlich motiviert ist.[157] Im Fall LiveUniverse v. MySpace hatte der Betreiber eines konkurrierenden sozialen Netzwerks MySpace beschuldigt, sich wettbewerbswidrig zu verhalten, indem es nicht zuließ, dass die Webseite des Konkurrenten von der MySpace-Webseite aus besucht wurde. Der Neunte Circuit Court wies die Beschwerde jedoch zurück: „LiveUniverse does not explain how MySpace's actions *on its own website* can reduce consumers' choice or diminish the quality of their experience on *other* social networking websites, which is the relevant market."[158] Schließlich hatte sich der District Court im Nördlichen Distrikt Kalifornien in der Sache Facebook v. Power Ventures mit einer Webseite zu befassen, die es den Nutzern erlaubt hätte, all ihre Kontakte aus sozialen Netzwerken in eine Webseite zu integrieren. Das Gericht befand jedoch, dass Facebook sich nicht wettbewerbswidrig verhielt, indem es Power Ventures keinen Zugang zu Facebook gewährte.[159] Die restriktive Haltung der Gerichte hinsichtlich der Anerkennung wettbewerbswidrigen Verhaltens erschwert zwar ein wettbewerbsrechtliches Vorgehen gegen mächtige Betreiber sozialer Netzwerke. Dennoch ist sie sachgerecht, da Investoren vom Aufbau neuer sozialer Netzwerke abgeschreckt würden, wenn sie, sobald sie Marktmacht erlangt haben, zur Kooperation mit ihren Wettbewerbern gezwungen und Gefahr laufen würden, dass sich ihre Investitionen aus diesem Grund nicht rentieren. Der Spielraum der Gerichte bei der Bejahung wettbewerbswidrigen Verhaltens wird jedenfalls begrenzt durch die deutschen Wirtschaftsgrundrechte beziehungsweise die US-amerikanische Redefreiheit der Betreiber. Gerade Letztere stellt ein schwer überwindbares Hindernis dar.

Wie der Blick auf die Beispiele aus den USA zeigt, könnte das Kartellrecht durchaus dazu dienen, den Missbrauch einer marktbeherrschenden Stellung durch Anbieter von Internetangeboten zu verhindern.[160] Jedoch bedarf es dazu eines, bislang von den US-Gerichten noch nicht festgestellten, gravierend wettbewerbswidrigen Verhaltens. Ein solches wäre beispielsweise denkbar, wenn ein Anbieter eines sozialen Netzwerks es seinen Nutzern verbieten würde, Angebote eines Wettbewerbs zu nutzen.

Die EU-Kommission hat im April 2015 eine formelle Beschwerde an Google übermittelt.[161] Dem Konzern wird vorgeworfen, seine marktbeherrschende Stellung zu missbrauchen, indem er seinen eigenen Preisvergleichsdienst auf seinen allgemeinen Suchergebnisseiten systematisch bevorzugt. Des Weiteren läuft eine

---

157 Aspen Skiing Co. v. Aspen Highlands Skiing Corp., 472 U.S. 585 (1985). Einer darüber hinausgehenden generellen Verpflichtung zur Kooperation mit Wettbewerbern stünden auch wohl nicht überwindbare verfassungsrechtliche Bedenken entgegen, da Rechtfertigungsmöglichkeiten für einen derartig intensiven und pauschalen Eingriff in die Rechte der betroffenen Unternehmen nicht ersichtlich sind.

158 See LiveUniverse, Inc. v. MySpace, Inc., 304 Fed. Appx. 554, 557 (9th Cir. 2008) (Hervorhebungen im Original).

159 Facebook, Inc. v. Power Ventures, Inc., 2009 WL 1299698 (N.D. Cal. 2009).

160 Auf europäischer Ebene wären Art. 102 und 103 AEUV die Mittel für ein solches Vorgehen.

161 *Europäische Kommission*, Kartellrecht, 15.4.2015.

separate Untersuchung in Bezug auf Android Betriebssysteme, Anwendungen und Dienste für intelligente Mobilgeräte. Der weitere Verlauf der Verfahren bleibt abzuwarten.

2. Regulierte Selbstregulierung und ihre Durchsetzung im Wege des Rechts des unlauteren Wettbewerbs

Weiter bietet es sich an, in Ergänzung zur staatlichen Regulierung eine regulierte Selbstregulierung der verantwortlichen Stellen zu fördern und die Gewähr der Einhaltung der Selbstverpflichtungen im Wege des Rechts des unlauteren Wettbewerbs zu forcieren.

a) Regulierte Selbstregulierung

Informationeller Selbstschutz bedarf eines staatlichen Rahmens, der es den Nutzern insbesondere ermöglicht, die Praktiken der verantwortlichen Stellen einzuschätzen und eine informierte Entscheidung zwischen Wettbewerbern zu treffen.

Gerade angesichts der hohen Hürde, die die Rechte der verantwortlichen Stellen aus dem Ersten Zusatzartikel errichten, gestaltet sich die Verhinderung informationeller Preisgabe durch den Staat in den USA schwierig. Eine Alternative stellen Selbstverpflichtungen der Industrie dar. In den Vereinigten Staaten verfügt ein Großteil der Webseiten über häufig freiwillig aufgenommene Datenschutzrichtlinien (sogenannte Privacy Policies),[162] die Auskunft geben über die praktizierte Datenerhebung, -speicherung und -verarbeitung.

Um einen effektiven Schutz sicherzustellen, sind staatliche Interventionen dem bloßen Vertrauen auf den Markt vorzuziehen. Soweit eine Intervention allerdings nicht zulässig ist, erscheint es sinnvoll, auch in Deutschland gemäß dem US-Beispiel verstärkt auf, über das gesetzlich vorgeschriebene Maß hinausgehende,[163] Selbstverpflichtung zurückzugreifen. Ein effektives Konzept zu einer regulierten Selbstregulierung muss dabei bestehen aus der Unterstützung der Selbstregulierung, der Anerkennung der selbstgesetzten Regeln und deren freiwilliger, aber verbindlicher Geltung.[164]

---

[162] Ausführlich zum Wesen der Privacy Policies: *Schröder*, Die Haftung für Verstöße gegen Privacy Policies und Codes of Conduct nach US-amerikanischem und deutschem Recht, 2007, 21 ff.

[163] Die Auszeichnung der Einhaltung des gesetzlichen Niveaus erscheint hingegen insbesondere sinnvoll, wenn ein Markt gegeben ist, in dem die Kunden „von massenhaften Rechtsbrüchen der Anbieter ausgehen“, sodass schon die schlichte Einhaltung der gesetzlichen Vorgaben einen Wettbewerbsvorteil für die zertifizierten verantwortlichen Stellen bedeuten kann: *Hornung/Hartl*, Datenschutz durch Marktanreize – auch in Europa?, ZD 2014, 219, 221.

[164] Allgemein zu den verschiedenen Konzepten der Selbstregulierung: *Hoffmann-Riem*, Öffentliches Recht und Privatrecht als wechselseitige Auffangordnungen, in: Hoffmann-Riem/Schmidt-Aßmann (Hrsg.), Öffentliches Recht und Privatrecht als wechselseitige Auffangordnungen, 1996, 261, 300 ff.; *Holznagel*, Regulierte Selbstregulierung im Medienrecht, in: Die Verwaltung Beiheft 4, 2001, 81, 83 ff.; *Ladeur*, Die Regulierung von Selbstregulierung und die Herausbil-

Ein Anreiz zur Beteiligung an der Selbstregulierung und zur Einhaltung der, beispielsweise durch Branchenverbände ausgearbeiteten, Standards besteht insbesondere, wenn den verantwortlichen Stellen dadurch ein Wettbewerbsvorteil gegenüber Konkurrenten entsteht, die sich nicht zur Einhaltung der Datenschutzstandards verpflichtet haben. Die bloße Behauptung, selbst gesetzte Datenschutzstandards zu beachten, wird bei Nutzern zurecht auf Skepsis stoßen, da sie weder beurteilen können, wie privatheitsfreundlich die individuellen Standards sind, noch, ob die verantwortliche Stelle diese tatsächlich einhält. Es bedarf daher vielmehr einheitlicher, verlässlicher Gütesiegel, die die Beachtung einer in der Bevölkerung bekannten datenschutzrechtlichen Selbstverpflichtung belegen. Derartige Programme schaffen Transparenz und Vergleichbarkeit für die Nutzer und ermöglichen ihnen so die selbstbestimmte Entscheidung über die Aufgabe ihrer Privatheit.

Ein Weg zur Förderung dieser Form von Selbstregulierung ist die seit geraumer Zeit geforderte Zurverfügungstellung vertrauenswürdiger Audit- und Zertifizierungsprogramme. Im Rahmen eines Datenschutzaudits wird ein Verfahren der verantwortlichen Stelle geprüft, wohingegen sich die Zertifizierung auf ein bestimmtes IT-Produkt oder eine Dienstleistung bezieht.[165] Im Rahmen beider werden die Einhaltung der jeweiligen Datenschutzstandards rechtlich untersucht und entsprechende Siegel vergeben, sodass die Ergebnisse der Prüfung de jure abgesichert im Wettbewerb genutzt werden können.[166] In Deutschland ist die in § 9a BDSG angekündigte Gesetzgebung auf Bundesebene bislang im Sande verlaufen.[167] Erfolgreiches Vorbild für weitere Datenschutzaudits kann hingegen das European Privacy Seal[168] sein, das auf § 4 Abs. 2 Satz 2 Landesdatenschutzgesetz Schleswig-Holstein zurückgeht.

In Art. 39 EU-DS-GVO-E ist vorgesehen, dass die Mitgliedstaaten und die Kommission „die Einführung von datenschutzspezifischen Zertifizierungsverfahren so-

---

dung einer „Logik der Netzwerke“, in: Die Verwaltung Beiheft 4, 2001, 59 ff.; *Roßnagel/Pfitzmann/Garstka*, Modernisierung des Datenschutzrechts, DuD 2001, 253, 261; *dies.*, Modernisierung des Datenschutzrechts, 2001, 153 ff.; *Schulz*, Regulierte Selbstregulierung im Telekommunikationsrecht, in: Die Verwaltung Beiheft 4, 2001, 101, 108 ff.; *Schmidt-Aßmann*, Regulierte Selbstregulierung als Element verwaltungsrechtlicher Systembildung, in: Die Verwaltung Beiheft 4, 2001, 253, 254 ff.; zur Diskussion um ein Selbstregulierungsabkommen für soziale Netzwerke: *Dehmel*, Selbstregulierung, in: Hill/Martini/Wagner (Hrsg.), Facebook, Google & Co., 2013, 135 ff. Zu den verschiedenen Einsatzmöglichkeiten regulierter Selbstregulierung im Bereich des Datenschutzes sei verwiesen auf: *Talidou*, Regulierte Selbstregulierung im Bereich des Datenschutzes, 2005.

[165] Zur Unterscheidung beider, häufig gemeinsam erwähnter, Begriffe: *Hornung/Hartl*, Datenschutz durch Marktanreize – auch in Europa?, ZD 2014, 219 f.; grundlegend zur Konzeption des Datenschutzaudits: *Roßnagel*, Datenschutzaudit, 2000.

[166] *Roßnagel/Pfitzmann/Garstka*, Modernisierung des Datenschutzrechts, 2001, 132 ff. und *dies.*, Modernisierung des Datenschutzrechts, DuD 2001, 253, 255.

[167] Zur Diskussion um den Erlass eines Bundesauditgesetzes: *Hornung/Hartl*, Datenschutz durch Marktanreize – auch in Europa?, ZD 2014, 219, 222.

[168] Https://www.european-privacy-seal.eu/EPS-en/Home.

wie von Datenschutzsiegeln und -zeichen" fördern.[169] Die LIBE-Fassung des Entwurfs der EU-Datenschutz-Grundverordnung enthält weitere Details zur Einführung eines „European Data Protection Seal“ (Art. 39 Abs. 1e). Jedoch soll sich die Überprüfung nach beiden Entwürfen lediglich auf die Einhaltung der EU-Datenschutz-Grundverordnung beschränken (Art. 39 Abs. 1 Satz 2 EU-DS-GVO-E beziehungsweise Art. 39 Abs. 1a der LIBE-Fassung). Die Beachtung von hier vorgeschlagenen, über das gesetzlich vorgeschriebene Niveau hinausgehenden, Selbstverpflichtungen ist nicht erfasst.

In Ergänzung zu Datenschutzvorschriften und zu unternehmensinternen, nicht bindenden Datenschutzrichtlinien ist die Entwicklung von Datenschutzverhaltenskodizes wünschenswert, denen sich die verantwortlichen Stellen freiwillig unterwerfen. Diese könnten insbesondere Regelungen zur Verhinderung von Preisgabe enthalten, die die Preisgebenden oder das Allgemeinwohl gefährdet. Sinnvoll erscheint es, dass sich verantwortliche Stellen beispielsweise zum Einsatz von Entscheidungsarchitekturen verpflichten, um vorhersehbaren Rationalitätsdefiziten der Nutzer entgegenzuwirken. Die Selbstverpflichtungen sollten auch durch die Nachfrage der Nutzer nach privatheitsschonenden Internetdiensten angestoßen werden. Der Staat kann solche Entwicklungen anregen, die Verantwortung liegt jedoch bei den verantwortlichen Stellen und – indirekt über ihre Marktmacht – bei den Preisgebenden.

b) Durchsetzung im Wege des Rechts des unlauteren Wettbewerbs

Auch wenn keine gesetzliche Pflicht zur Einhaltung eingegangener Selbstverpflichtungen besteht, können Verstöße gegen sie dennoch rechtliche Folgen nach sich ziehen.

Die Einhaltung der Datenschutzrichtlinien der verantwortlichen Stellen wird in den USA mittelbar durch die Federal Trade Commission sichergestellt:[170] Sobald ein Unternehmen eine Datenschutzrichtline veröffentlicht, überwacht die Federal Trade Commission deren Einhaltung. Allerdings bezieht sich dies nicht auf ein allgemein vorgegebenes, sondern strikt nur auf das selbst gewählte Datenschutzniveau. So gäbe auch eine Datenschutzrichtlinie mit dem Inhalt „Wir geben alle Daten an beliebige Dritte weiter“ keinen Anlass zu einer Beanstandung durch die Federal Trade Commission. Sobald jedoch das tatsächliche Verhalten negativ von dem in der Datenschutzrichtlinie versprochenen Gebaren abweicht, kann ein unlauteres Verhalten in Form von „unfair and deceptive acts and practices in or affecting commerce“ vorliegen,[171] sodass die Federal Trade Commission dagegen einschreiten

---

[169] Eine Analyse der aktuellen europarechtlichen Diskussion bieten: *Hornung/Hartl*, Datenschutz durch Marktanreize – auch in Europa?, ZD 2014, 219, 223 ff.

[170] Ausführlich zur Durchsetzung von Privacy Policies durch die Federal Trade Commission: *Schröder*, Die Haftung für Verstöße gegen Privacy Policies und Codes of Conduct nach US-amerikanischem und deutschem Recht, 2007, 81 ff.

[171] 15 U.S.C. § 45.

kann.[172] Grundlage ist das Vertrauen darein, dass Bürger ihre Rechte selbst wahren, solange sie nur auf zutreffender Tatschengrundlage entscheiden können.[173]

Obwohl kein kodifiziertes sektorenübergreifendes Datenschutzrecht besteht, gehen aufgrund der Durchsetzungskraft der Federal Trade Commission jedenfalls viele US-amerikanische Stimmen von einem, auch im Vergleich zur Europäischen Union, wirksamen Datenschutz aus.[174] Dieser Einschätzung ist zwar zuzugestehen, dass der Einfluss der Federal Trade Commission signifikant ist. Da der Schutz in weiten Teilen nicht inhaltlich vorgegeben ist, ist er aber nur fragmentarischer Natur und insbesondere häufig ausgeschlossen, solange die verantwortlichen Stellen nicht gegen ihre eigenen Versprechen verstoßen. Das europäische Datenschutzniveau wird daher sicherlich nicht erreicht.

Trotzdem erscheint es ein sinnvoller Weg, in Anlehnung an das Vorgehen der Federal Trade Commission einen Verstoß gegen Selbstverpflichtungen auch in Deutschland mittels des Rechts des unlauteren Wettbewerbs zu sanktionieren und so über den ausdrücklich gesetzlich gewährten Privatheitsschutz hinaus den Gefahren informationeller Preisgabe zu begegnen.

Sachgerecht ist es, Verbraucherschutzorganisationen durch Gesetz, wie beispielsweise in Art. 73 EU-DS-GVO-E vorgeschlagen, oder Gesetzesauslegung ein Verbandsklagerecht einzuräumen, um Verstöße gegen Datenschutzverpflichtungen gerichtlich ahnden zu können.[175] Anlass für eine grundlegende Neustrukturierung des Rechts des unlauteren Wettbewerbs besteht nicht, vielmehr kann auf bestehende Strukturen aufgebaut werden. Auseinanderzuhalten sind vier ähnliche Konstellationen, von denen nur die letztgenannte den Fall der Selbstregulierungen betrifft:

Zunächst haben Diensteanbieter nach § 13 Abs. 1 Satz 1 TMG die Nutzer über Art, Umfang und Zwecke der Erhebung und Verwendung ihrer personenbezogenen Daten zu unterrichten. Weicht der Inhalt dieser Unterrichtung von den gemäß §§ 14 f. TMG zulässigen Praktiken ab, kann dies eine unangemessene Benachteiligung im Sinne des § 307 BGB darstellen, sodass ein Unterlassungsanspruch nach § 1 UKlaG besteht, der von Verbraucherschutzverbänden geltend gemacht werden kann (§ 3 Abs. 1 Nr. 1 UKlaG). Von der Einordnung der Datenschutzrichtlinien als

---

[172] Der Consumer-Data-Privacy-in-a-Networked-World-Report des Weißen Hauses fordert noch weitergehende Kompetenzen der Federal Trade Commission: *The White House*, Consumer Data Privacy in a Networked World, 2.2012, 36.

[173] *Nehf*, Shopping for Privacy Online, 1 Univ. of Illinios J. of L., Tech. and Policy (2005), 1, 4.

[174] *Bamberger/Mulligan*, Privacy on the Books and on the Ground, 63 Stanford L. Rev. Online (2011), 247, 273 ff. m. w. N.; *The White House*, Consumer Data Privacy in a Networked World, 2.2012, 42. Eine hilfreiche Systematisierung der Datenschutz-relevanten Fälle der Federal Trade Commission bietet das jüngst vorgestellte FTC Privacy Casebook der International Association of Privacy Professionals: https://privacyassociation.org/resources/ftc-casebook/.

[175] So auch: *Schneider/Härting*, Datenschutz in Europa, CR 2014, 306, 311; a. A.: *Nietsch*, Zur Überprüfung des Datenschutzrechts durch Verbraucherverbände, CR 2014, 272, 277 f., da diese Aufgabe den Datenschutzbehörden vorbehalten bleiben sollte, um eine Rechtszersplitterung zu verhindern.

Allgemeine Geschäftsbedingungen wird – trotz gegenteiliger Stimmen[176] – auszugehen sein.[177] Da sich diese Konstellation jedoch nur mit Fällen beschäftigt, in denen gegen die gesetzlichen Datenschutzbestimmungen der §§ 14 f. TMG verstoßen wird, bleibt sie hier außen vor.

Weiter könnten Verstöße gegen die Datenschutzvorschriften insbesondere des Bundesdatenschutzgesetzes und des Telemediengesetzes einen Unterlassungsanspruch der Verbraucherschutzorganisationen begründen, wenn die Datenschutzgesetze Verbraucherschutzgesetze im Sinne des § 2 Abs. 1 Satz 1 UKlaG darstellen. § 2 Abs. 2 UKlaG enthält eine beispielhafte Aufzählung von Verbraucherschutzgesetzen, ohne jedoch Datenschutzvorschriften zu erwähnen. Derzeit ist nicht davon auszugehen, dass Datenschutzgesetze als Verbraucherschutzgesetze zu werten sind, da sie nicht vorrangig dem Schutz von Verbrauchern im Sinne des § 13 BGB dienen, sondern dem Schutz aller natürlichen Personen.[178] Um diese Lücke zu schließen, hat das Bundeskabinett Anfang 2015 einen Gesetzesentwurf beschlossen, der Verbraucherverbänden ein Verbandsklagerecht bei Datenschutzverstößen einräumen soll.[179]

Zudem könnten Verstöße gegen Datenschutzgesetze Verbraucherverbänden auch ein Klagerecht nach § 8 Nr. 3 UWG geben, wenn das verletzte Datenschutzgesetz „auch dazu bestimmt ist, im Interesse der Marktteilnehmer das Marktverhalten zu regeln“ (§ 4 Nr. 11 UWG). Da Datenschutzgesetze jedoch primär dem Schutz der informationellen Selbstbestimmung der Betroffenen dienen, ist ohne Klarstellung des Gesetzgebers davon auszugehen, dass kein ausreichender Marktbezug vorliegt.[180] Soweit die Selbstverpflichtung lediglich die Einhaltung der gesetzlichen

---

[176] Datenschutzerklärungen könnten nicht als Allgemeine Geschäftsbedingungen eingeordnet werden, da die Diensteanbieter nach §§ 14 f. TMG zur Abgabe der Erklärungen verpflichtet sind und ihnen daher eher ein deklarativer Charakter zukommt: *Nietsch*, Zur Überprüfung des Datenschutzrechts durch Verbraucherverbände, CR 2014, 272, 274 ff. *Köpernik* weist trotz Zustimmung zur Einordnung der Datenschutzrichtlinien als Allgemeine Geschäftsbedingungen zurecht darauf hin, dass verantwortliche Stellen, die über widerrechtliche Datenverwendung in ihren Datenschutzerklärungen aufklären (bei Anerkennung der Datenschutzerklärungen als Allgemeine Geschäftsbedingungen) schlechter stehen als wenn sie gar nicht aufgeklärt hätten: *Köpernik*, Zur Notwendigkeit einer Verbandsklage bei Datenschutzverstößen, VuR 2014, 240, 242.

[177] Diese Einschätzung scheint der deutsche Bundesjustizminister *Maas* zu teilen: *Bundesministerium der Justiz und für Verbraucherschutz*, Mailen, Surfen, Chatten – Wie ist die Privatsphäre zu retten?, 11.2.2014; so auch: *Köpernik*, Zur Notwendigkeit einer Verbandsklage bei Datenschutzverstößen, VuR 2014, 240 und *Weichert*, Datenschutz im Wettbewerbs- und Verbraucherrecht, VuR 2006, 377, 382.

[178] So auch: OLG Frankfurt am Main, NJW-RR 2005, 1280, 1281 (zu § 28 BDSG); *Nietsch*, Zur Überprüfung des Datenschutzrechts durch Verbraucherverbände, CR 2014, 272, 277; offen gelassen durch: *Köpernik*, Zur Notwendigkeit einer Verbandsklage bei Datenschutzverstößen, VuR 2014, 240 ff.; a. A.: *Weichert*, Datenschutz im Wettbewerbs- und Verbraucherrecht, VuR 2006, 377, 382.

[179] *Redaktion beck-aktuell*, Gesetzentwurf: Kabinett beschließt Verbandsklagerecht bei missbräuchlicher Verwendung von Verbraucherdaten, 4.2.2015 becklink 1036989; zu den Hintergründen: *Bundesministerium der Justiz und für Verbraucherschutz*, Mailen, Surfen, Chatten – Wie ist die Privatsphäre zu retten?, 11.2.2014.

[180] Ob das Datenschutzrecht Marktverhaltensregeln enthält, ist umstritten. Ablehnend ent-

Bestimmungen zum Gegenstand hat, kann auch diese zweite Konstellation für die vorliegende Arbeit außer Betracht bleiben.

Das Augenmerk soll vielmehr auf einer vierten Situation liegen: Der Kontrolle von freiwilligen Selbstverpflichtungen, die über das gesetzliche Schutzniveau hinausgehen. Basis dafür kann § 5 Abs. 1 UWG sein:

Nach § 5 Abs. 1 Satz 2, 2. Alt. Nr. 6 UWG liegt eine irreführende geschäftliche Handlung vor, wenn diese zur Täuschung geeignete Angaben über die Einhaltung eines Verhaltenskodex enthält, auf dessen Beachtung sich der Unternehmer verbindlich verpflichtet hat und er auf diese Bindung hinweist. Unter einem Verhaltenskodex ist in richtlinienkonformer Auslegung eine Vereinbarung oder ein Vorschriftenkatalog zu verstehen, die beziehungsweise der über das rechtlich Vorgeschriebene hinausgeht und das Verhalten der Gewerbetreibenden definiert, die sich in Bezug auf eine oder mehrere spezielle Geschäftspraktiken oder Wirtschaftszweige auf diesen Kodex verpflichten.[181] Unterwirft sich eine verantwortliche Stelle erstens freiwillig einem verbindlichen Datenschutzkodex, der zweitens über die gesetzlichen Vorschriften hinaus Datenschutz vorschreibt und weist die verantwortliche Stelle drittens explizit auf diese Bindung hin, kann bei Nichtbeachtung des Datenschutzkodexes eine irreführende geschäftliche Handlung vorliegen. Diese muss jedoch viertens zur Täuschung geeignet, also in der Lage sein, die geschäftliche Entscheidung der Verbraucher zu beeinflussen oder aus diesem Grund Mitbewerber zu behindern.[182] Vielen Nutzern liegt an der Wahrung ihrer Privatheit, sodass der Hinweis auf die Einhaltung eines Datenschutzkodex ihre Entscheidung für einen Wettbewerber beeinflussen kann.

Zudem stellt ein systematischer Verstoß gegen Selbstverpflichtungen eine „unwahre Angabe" und damit eine irreführende geschäftliche Handlung im Sinne des § 5 Abs. 1 Satz 2, 1. Alt. UWG dar, wenn der Unternehmer mit der Einhaltung der Selbstverpflichtungen wirbt.[183]

---

schied das Oberlandesgericht München hinsichtlich §§ 4a Abs. 1, 28 Abs. 1 Nr. 3, 35 Abs. 2, 3 BDSG, OLG München GRUR-RR 2012, 395 (396); so auch: *Nietsch*, Zur Überprüfung des Datenschutzrechts durch Verbraucherverbände, CR 2014, 272, 277 und *Nink/Laue*, Anmerkung zu LG Frankfurt/M., CR 2014, 269 f. Das Landgericht Frankfurt am Main hingegen entschied jüngst, dass § 15 Abs. 3 TMG eine marktverhaltensregelnde Vorschrift im Sinne des § 4 Nr. 11 UWG darstellt, LG Frankfurt/Main, CR 2014, 266 (268 f.). Das Kammergericht entschied, dass §§ 4a Abs. 1, 28 Abs. 3 Nr. 1 BDSG die Eigenschaft als Marktverhaltensregel zukommt, KG CR 2014, 319; zur Frage, welchen datenschutzrechtlichen Regeln im Einzelnen Marktrelevanz zukommt: *Weichert*, Datenschutz im Wettbewerbs- und Verbraucherrecht, VuR 2006, 377, 380 ff.

[181] So die Definition von Art. 2 lit. f Richtlinie über unlautere Geschäftspraktiken, RL 2005/29/EG v. 11.5.2005.

[182] *Dreyer*, in: Harte-Bavendamm/Henning-Bodewig (Hrsg.), Gesetz gegen den Unlauteren Wettbewerb, 2013, § 5 Abs. 1 Satz 2 Nr. 6, Rn. 7.

[183] Zu diesem Ergebnis kommt auch die Tagung des Max-Planck-Instituts für Geistiges Eigentum, Wettbewerbs- und Steuerrecht zum Thema „Corporate Social Responsibility im Lauterbarkeitsrecht" v. 16./17.5.2013, vgl. die Darstellung der Ergebnisse durch: *Augsburger*, Lauterkeitsrechtliche Beurteilung von Corporate Responsibility Codes, MMR 2014, 427, 428 f.

Verstöße gegen Selbstverpflichtungen können dann, wenn sie zulasten der Verbraucher gehen, in beiden Fällen einen Verstoß gegen § 3 Abs. 1, 2 in Verbindung mit § 5 Abs. 1 Satz 2 UWG darstellen. Verbraucherschutzverbänden können daher nach § 8 Abs. 3 Nr. 3 UWG Beseitigungs- und Unterlassungsansprüche sowie nach § 10 Abs. 1 UWG Gewinnabschöpfungsansprüche zustehen. Abhängig von der Entwicklung der europäischen Datenschutzreform könnte solche Verstöße auch mittels des in Art. 73 EU-DS-GVO-E vorgeschlagenen Verbandsklagerechts geltend gemacht werden.

3. Gestärkte Eigenverantwortung der Nutzer

Schließlich gibt es viele Situationen, in denen dem Staat nicht zwingend die Rolle des „Beschützers" zukommen sollte. Paternalistische Maßnahmen führen immer auch dazu, dass den Bürgern Entscheidungen abgenommen werden. Dadurch werden sie in gewisser Weise aus ihrer ethischen Obliegenheit zu moralisch gutem und verantwortungsbewusstem Verhalten entlassen.[184] Dies wiederum kann, auf lange Sicht gesehen, dazu führen, dass sie weniger über ihr Handeln reflektieren und so ein gesamtgesellschaftlicher Nachteil entsteht.

Das liberale US-System kann als Beispiel dafür dienen, auch in Deutschland mehr Vertrauen in die Nutzer zu setzen und ihnen zugleich mehr Verantwortung aufzuerlegen. Den Gefahren informationeller Preisgabe kann begegnet werden, wenn nicht gegen den Willen von Preisgebenden und verantwortlichen Stellen Schutz aufoktroyiert wird, sondern die Nutzer als Marktteilnehmer selbstbestimmte informationelle Preisgabe praktizieren und sich für privatheitsfreundliche Anbieter entscheiden, soweit dies ihren Präferenzen entspricht. Privatheitswahrung kann damit zum Unique Selling Point für Unternehmen werden.[185]

Die Verantwortung der Nutzer erstreckt sich dabei jedoch nur auf deren selbstbestimmte informationelle Preisgabe und auch dies nur, soweit nicht die Allgemeinheit zu Schaden kommt. Unter diesen Voraussetzungen mag es häufig tatsächlich rechtspolitisch wünschenswert sein, auf eine staatliche Intervention zu verzichten. Leitend kann das Motto sein: „happy to trust free individuals to make their own welfare decisions and let them live with the consequences."[186]

---

[184] *Diggelmann*, Grundrechtsschutz der Privatheit, in: Höfling (Hrsg.), Der Schutzauftrag des Rechts, 2011, 50, 57, Fn. 23.

[185] Dies wird freilich primär dann einen Unterschied machen, wenn es um „funktional im Wesentlichen gleichwertige Angebote" geht: *Hornung*, Europa und darüber hinaus, in: Hill/Schliesky (Hrsg.), Die Neubestimmung der Privatheit, 2014, 123, 147.

[186] *Mitchell*, Libertarian Paternalism Is an Oxymoron, 5.2002 FSU College of Law, Law and Economics Paper, 1, 31.

C. Gemeinsame Forschung und gemeinsame Standards

Trotz unterschiedlicher rechtlicher Systeme zeigt sich, dass Deutschland und die Vereinigten Staaten mit identischen Gefahren informationeller Preisgabe konfrontiert sind und zu deren Verhinderung auf einen vergleichbaren Maßnahmenkatalog zurückgreifen können. Unabhängig davon, ob die Durchsetzung primär durch Gesetz oder im Wege der Selbstverpflichtung erfolgt, lohnt es daher, die gemeinsame Forschung voranzutreiben (beispielsweise in den Bereichen des Privacy by Design oder der Entscheidungsarchitekturen) und sich auf gemeinsame Standards zu einigen.

So ist es beispielsweise sinnvoll, einen gemeinsamen Do-not-track-Standard festzulegen. In Deutschland könnte das Setzen eines Do-not-track-Befehls als Ablehnung der Einwilligung zur Datenerhebung gewertet werden. In den Vereinigten Staaten hingegen könnte die Einhaltung der Do-not-track-Präferenzen der Nutzer durch die Federal Trade Commission kontrolliert werden, wenn sich die verantwortlichen Stellen in ihren Datenschutzrichtlinien zur Beachtung von Do-not-track-Befehlen verpflichten. Trotz unterschiedlicher Durchsetzungswege im innerstaatlichen Recht wären damit für international agierende Unternehmen praktikable Wege zum Privatheitsschutz und eine größere Rechtssicherheit als bisher gewährleistet. Schwierigkeiten stellen sich allerdings bei der Frage, in welchem Forum der erforderliche Dialog sinnvollerweise stattfinden kann. Denkbar erscheint es beispielsweise, solche Annäherungen im Rahmen des Internet Governance Forums zu erreichen.

Zudem ist zu beachten, dass von Anforderungen in einer Rechtsordnung eine über das eigene Territorium hinausgehende Ausstrahlungswirkung ausgeht. Bereits jetzt scheint sich beispielsweise eine große Zahl der Webseitenanbieter in den Vereinigten Staaten nach den einzelstaatlichen Vorgaben des California Online Privacy Protection Act (CalOPPA) zu richten, der die Existenz von näher bestimmten Datenschutzrichtlinien fordert, sobald eine Webseite personenbezogene Daten von kalifornischen Bürgern sammelt, die diese Webseite besuchen.[187]

Eine ähnliche Ausstrahlungswirkung kann die verbindliche Implementierung datenschutzrechtlicher Standards jedenfalls auf EU-Ebene haben, selbst wenn diese Standards in den Vereinigten Staaten nur den Status einer Selbstverpflichtung erreichen. Einen Beitrag zur Herstellung von Rechtssicherheit soll die geplante EU-Datenschutz-Grundverordnung[188] leisten. Aufgrund ihrer extraterritorialen Anwend-

---

[187] Online Privacy Protection Act of 2003, Sec. 22575-22579.

[188] Zur Diskussion um den EU-DS-GVO-E: *Hert/Papakonstantinou*, The proposed data protection Regulation replacing Directive 95/46/EC, 28 Computer Law & Security Review (2012), 130 ff.; *Hornung*, Eine Datenschutzgrundverordnung für Europa?, ZD 2012, 99 ff. und *Knyrim*, Entwurf der neuen EU-Datenschutz-Grundverordnung, in: Scholz/Funk (Hrsg.), DGRI Jahrbuch 2012, 2013, 25 ff. Einen Einblick in die Einflussnahme von Lobbyisten auf den EU-DS-GVO-E bietet: http://lobbyplag.eu/influence. Dort werden systematisch Textstellen gelistet, die aus Lob-

barkeit (Art. 3 EU-DS-GVO-E), der empfindlichen Sanktionsmechanismen (Art. 79 EU-DS-GVO-E: nach der LIBE-Fassung bis zu 100 Millionen Euro oder fünf Prozent des Jahresumsatzes eines Unternehmens) und des großen erfassten Wirtschaftsraums besteht Hoffnung, dass in der Europäischen Union gesetzte Standards aus Praktikabilitätsgründen auch in den Vereinigten Staaten und anderorts übernommen werden oder zumindest Annäherungsprozesse auslösen. Ihre Einhaltung wiederum kann in den USA im Falle entsprechender Selbstverpflichtungen durch die Federal Trade Commission sichergestellt werden. Die faktische Bedeutung der EU-Datenschutz-Grundverordnung für die Vereinigten Staaten wird in der dortigen Forschung groß eingeschätzt, wie sich an einer Vielzahl entsprechender Publikationen aus den vergangenen Jahren zeigt.[189]

Einen weiteren Beitrag zur jedenfalls teilweisen Annäherung von Datenschutzstandards zwischen Europa und den Vereinigten Staaten kann eine überarbeitete Fassung des umstrittenen und derzeit dem Europäischen Gerichtshof vorgelegten[190] Safe Harbor-Abkommens leisten. US-amerikanische Unternehmen könnten sich zur Einhaltung bestimmter von der Europäischen Union vorgegebener Standards verpflichten und die Europäische Union im Gegenzug Datentransfers zu diesen Unternehmen erlauben. Einen weiteren interessanten, wenn auch wohl schwer umzusetzenden, Vorschlag enthält Art. 42 Nr. 2 (aa) der LIBE-Fassung der EU-Datenschutz-Grundverordnung: Datentransfers in Drittstaaten sollen zulässig sein, wenn sich der Absender in der Europäischen Union und der Empfänger im Drittstaat einem Datenschutzaudit unterzogen haben. Wenn tatsächlich ein Weg geschaffen wird, Empfänger außerhalb der Europäischen Union zu auditieren und diese Möglichkeit auch genutzt wird, wird dies zur Verbreitung europäischer Privatheitsstandards beitragen.

Angesichts der rasant fortschreitenden technischen Entwicklungen und der Omnipräsenz internetbasierter Anwendungen im Alltagsleben besteht sowohl in Deutschland als auch in den Vereinigten Staaten das rechtspolitische Bedürfnis, informationelle Preisgabe einzudämmen, wenn von ihr zu viele Gefahren ausgehen.

Dabei liegt beiden Rechtsordnungen ein sehr unterschiedliches Privatheitsverständnis zugrunde. Mehr denn je ist der Dialog in Wissenschaft, Praxis und Politik beider Länder gefragt, um bestmögliche, länderübergreifend geltende Ziele, Lösungen und Standards zu etablieren.

---

by-Dokumenten in Änderungsanträge zum EU-DS-GVO-E übernommen wurden; dazu: *Kuhn*, „Lobbyplag.eu“ zum Datenschutz, 11.2.2013.

[189] Beispielsweise *Rotenberg/Jacobs*, Updating the Law of Information Privacy, 36 Harvard J. of L. and Public Policy (2013), 606 ff.; *Schwartz*, The EU-U.S. Privacy Collision, 126 Harvard L. Rev. (2013), 1 ff.; *Tene/Wolf*, Overextended: Jurisdiction and Applicable Law under the EU General Data Protection Regulation, 2.2013.

[190] *Jensen*, Irischer High Court legt EuGH Fragen zum Safe Harbor-Abkommen vor, ZD-Aktuell 2014, 04284. Die mündliche Verhandlung fand am 24.3.2015 statt, *Redaktion ZD-Aktuell*, EuGH: Terminhinweis ZD-Aktuell 2015, 04593.

Denn um mit *Cohens* Worten zu sprechen: „Informational privacy is an essential building block for the kind of individuality, and the kind of society, that we say we value.“[191] Diesen Baustein gilt es zu schützen.

[191] *Cohen*, Examined Lives, 52 Stanford L. Rev. Online (2000), 1373, 1435.

Kapitel 8

Schlussbetrachtung

Informationelle Privatheit wird gerade im Internetkontext aus verschiedensten Gründen von Nutzern selbst langfristig preisgegeben. Die dadurch entstehenden Probleme stellen sich weltweit. Aus deutscher Sicht lohnt ein Blick auf die USA, die zum einen Standort der maßgeblichen Akteure im Markt der Internetanbieter sind und zum anderen einen deutlich anderen rechtlichen Rahmen für die Verhinderung informationeller Preisgabe bieten.

A. Zusammenfassende Thesen

Die gewonnen Erkenntnisse lassen sich wie folgt zusammenfassen:

I. Informationelle Preisgabe

– Informationelle Preisgabe ist die langfristige Aufgabe informationeller Privatheit durch die Privatheitsträger selbst.

– Informationelle Privatheit ist ein Aspekt der Privatheit. Privatheit dient der Sicherung der individuellen Autonomie und erfasst alles, was ihre Träger aus beliebigen Gründen nicht zeigen möchten. Die Unterkategorie informationelle Privatheit wird verstanden als die Möglichkeit der Einzelnen, selbst über die Preisgabe und Verwendung der eigenen personenbezogenen Daten zu bestimmen.

– Die Preisgabe informationeller Privatheit stellt ein aktives Handeln der Privatheitsträger dar, mit dem sie die Kontrolle über ihre personenbezogenen Daten aufgeben. Gesetzlich autorisierte sowie von vornherein rechtswidrige Datenerhebungen sind nicht erfasst, da sie unabhängig vom Willen der Nutzer erfolgen. Auf die Rationalität der Preisgabe kommt es nicht an. Sie kann explizit oder implizit erfolgen. Unter expliziter Preisgabe ist eine bewusste und zielgerichtete Preisgabe zu verstehen. Unter impliziter Preisgabe wird eine solche verstanden, die technisch im Hintergrund anlässlich der Nutzung von Internetangeboten, häufig unbewusst und ohne intentionales Zutun der Preisgebenden erfolgt.

II. Gefährdete Rechtsgüter

– Informationelle Preisgabe kann dazu führen, dass Nutzer auf Dauer gesehen ihre informationelle Privatheit einbüßen und in der Folge Selbstzensur hinsichtlich der Quellenauswahl und des Erkenntnisprozesses üben.

Im deutschen (Art. 2 Abs. 1 in Verbindung mit Art. 1 Abs. 1 GG) und im europäischen Recht (Art. 7 und 8 GR-Ch, Art. 8 EMRK) kommt der informationellen Privatheit der Nutzer ein hoher Rang zu. Dabei tangiert schon eine bloße Angst davor, die Kontrolle über die eigenen Daten zu verlieren und einer Überwachung ausgesetzt zu sein, die geschützten Interessen am Erhalt der informationellen Privatheit.

In den Vereinigten Staaten erfährt die informationelle Privatheit grundsätzlich Schutz durch den Vierten Zusatzartikel sowie die Due-Process-Klauseln. Jedoch greift der Schutz des Vierten Zusatzartikels neben anderen Einschränkungen gemäß der Third-Party-Doktrin nicht, sobald die Preisgebenden ihre Daten irgendjemandem anvertraut haben. Da Preisgabe im Internet technisch voraussetzt, dass Daten an andere Menschen oder Geräte übermittelt werden, bietet der Vierte Zusatzartikel regelmäßig keinen Schutz. Weiter kann die informationelle Privatheit durch die Due-Process-Klauseln abgesichert werden. In eng begrenzten Fällen wurde informationelle Privatheit als Fundamental Right anerkannt, sodass sie nur unter Wahrung substanzieller Rechtsstaatlichkeit eingeschränkt werden kann. Diese Fälle sind jedoch nicht verallgemeinerungsfähig. Zudem wird diskutiert, die Third-Party-Doktrin auch auf das Right to Informational Privacy zu übertragen und damit den Schutz durch das substanzielle Rechtsstaatlichkeitsgebot entfallen zu lassen, wenn die Daten irgendeinem Dritten anvertraut wurden. Regelmäßig erfährt informationelle Privatheit in den USA daher nur minimalen Schutz durch das allgemeine prozessuale Rechtsstaatlichkeitsgebot. Selbst wenn die befürchteten Gefahren nicht durch Private, sondern direkt durch den Staat ausgelöst würden, ist anzunehmen, dass kein verfassungsrechtlicher Schutz bestünde.

Die abweichende verfassungsrechtliche Bewertung lässt sich vor dem Hintergrund der unterschiedlichen Verfassungs- und Gesellschaftstraditionen begreifen. Das Recht auf informationelle Selbstbestimmung nach deutschem Verständnis schützt persönliche Würde und individuelle Selbstentfaltung. Privacy hingegen schützt in den USA als Recht, in Ruhe gelassen zu werden, die Individualinteressen der Einzelnen. Schutzobjekt ist die persönliche Freiheit vor dem Staat, insbesondere im eigenen Heim.

– Informationelle Preisgabe kann dazu führen, dass Nutzern keine neutrale Quellenauswahl zur Verfügung steht oder sie vor dem Aufrufen kontroverser Quellen zurückschrecken.

Die Informationsfreiheit im Sinne des Grundgesetzes (Art. 5 Abs. 1 Satz 1 Halbsatz 2 GG) und ihre europarechtlichen Pendants (Art. 10 Abs. 1 Satz 2, 2. Alt. EMRK; Art. 11 Abs. 1 Satz 2, 2. Alt. GR-Ch) schützen davor, durch den Staat von dem ungehinderten Zugang zu Informationen abgehalten zu werden. Werden Nut-

zer durch eine Vorselektion der Quellen oder durch Selbstzensur hinsichtlich der Quellenauswahl am freien Zugang zu Informationen gehindert, werden Interessen berührt, die durch die Informationsfreiheit geschützt sind. Sind Grundrechte verschiedener Grundrechtsträger in praktische Konkordanz zu bringen, findet in Deutschland regelmäßig eine gleichberechtigte Abwägung zwischen der Informationsfreiheit und den widerstreitenden Interessen statt.

In den Vereinigten Staaten wird das Recht, sich ohne Einflussnahme und uneingeschüchtert im Internet informieren zu können, vom Ersten Zusatzartikel geschützt. Diesem kommt im US-Verfassungssystem eine wichtige Rolle zu, bei der Herstellung praktischer Konkordanz setzt er sich regelmäßig gegen alle anderen Belange durch. Grund dafür ist die überragende Bedeutung, die der freie Fluss von Informationen im US-Rechtssystem innehat.

– Durch die Preisgabe kann die informationelle Privatheit Dritter gefährdet werden, wenn die preisgegebenen Daten Rückschlüsse auf die Dritten zulassen.

Die informationelle Privatheit Dritter wird in Deutschland durch das Recht auf informationelle Selbstbestimmung (Art. 2 Abs. 1 in Verbindung mit Art. 1 Abs. 1 GG) geschützt.

In den Vereinigten Staaten erfolgt der Schutz durch den Vierten Zusatzartikel beziehungsweise das Right to Privacy. Jedoch treten die Privatheitsinteressen Dritter regelmäßig hinter der Redefreiheit der Preisgebenden zurück, sobald es zu einer Abwägung kommt.

Insofern besteht in den Vereinigten Staaten zwar ein Schutz der informationellen Privatheit Dritter, jedoch bei Weitem nicht auf dem deutschen Niveau.

– Informationelle Preisgabe kann im Wege der Beeinträchtigung der Quellenauswahl sowie der Selbstzensur hinsichtlich der Quellenauswahl und des Erkenntnisprozesses den gesamtgesellschaftlichen Fortschritt in seinen drei Teilaspekten kultureller, wissenschaftlicher und wirtschaftlicher Fortschritt hemmen.

Dieser genießt in beiden Staaten gleichermaßen Verfassungsrang.

– Die Funktionsfähigkeit der Demokratie kann durch informationelle Preisgabe gefährdet werden, da die Bürger die Fähigkeit zum Erkennen notwendiger Veränderungen verlieren können, es ihnen an der erforderlichen Selbstbestimmung fehlen kann und sie schließlich von politischer Teilnahme abgeschreckt werden können.
Beide Verfassungen schützen vor den aufgezählten Gefahren durch individuelle Grundrechte. Zudem anerkennen sie generell den hohen Stellenwert der Demokratie. Angesichts des Bezugs zwischen Demokratie und der, gerade in den USA sehr starken, Meinungsfreiheit, könnte dem Schutz der Demokratie in den Vereinigten Staaten in Zukunft ein erhebliches Gewicht in der dogmatischen Entwicklung des Privatheitsschutzes zukommen, während sie im deutschen Recht wohl sekundär bleiben wird.

III. Mögliche Maßnahmen zur Verhinderung der Preisgabe

– In Deutschland und in den Vereinigten Staaten kann in tatsächlicher Hinsicht mit identischen Maßnahmen auf die Gefahren informationeller Preisgabe reagiert werden.

– Die möglichen Maßnahmen lassen sich grob unterteilen in einen erzwungenen Schutz (also Verbote und die Verhinderung durch Technikgestaltung), die Unterstützung informationellen Selbstschutzes (also insbesondere Unterrichtung und technische Selbstschutzmöglichkeiten) und Entscheidungsarchitekturen (also Ausnutzung vorhersehbarer kognitiver Anomalien bei der Entscheidung über die Preisgabe). Die Grenzen sind jedoch fließend.

IV. Pflicht zur Verhinderung der Preisgabe

– Die deutschen Grundrechte beinhalten eine objektiv-rechtliche Grundrechtsdimension. Aus ihnen können sich Pflichten zum Schutz Einzelner vor privaten Übergriffen ergeben.

Selbstbestimmt Preisgebenden fehlt es an der Schutzbedürftigkeit, selbst dann, wenn durch die Preisgabe der Menschenwürdekern des Rechts auf informationelle Selbstbestimmung berührt wird. Jedoch besteht eine Schutzpflicht zur Sicherung der Selbstbestimmung. Diese kann erfüllt werden durch Maßnahmen zur Unterstützung informationellen Selbstschutzes sowie nachrangig durch Entscheidungsarchitekturen.

Weiter muss erzwungener Schutz angewandt werden, um nicht selbstbestimmte Preisgabe zu verhindern.

Schließlich kann eine Schutzpflicht hinsichtlich der Rechte Dritter bestehen, wenn sich die Belange der durch die Preisgabe beeinträchtigten Dritten gegen die Grundrechte der Preisgebenden durchsetzen. Zwischen den widerstreitenden Grundrechten ist eine praktische Konkordanz herzustellen und ein geeignetes sowie erforderliches Mittel aus einer der drei Kategorien erzwungener Schutz, Unterstützung informationellen Selbstschutzes und Entscheidungsarchitekturen zu wählen. Regelmäßig wird der erzwungene Schutz das einzig wirksame Mittel sein. Hinsichtlich abstrakter Allgemeinwohlbelange besteht keine Schutzpflicht.

Gerade im Internetkontext entziehen sich die zugrunde liegenden Sachverhalte häufig dem Geltungsbereich des Grundgesetzes. Es gilt dann eine modifizierte Schutzpflicht, nach der sich der Staat um die Schaffung eines schützenden Rechtsrahmens auf europäischer oder völkerrechtlicher Ebene bemühen muss.

– Im Gegensatz zur deutschen Rechtslage kennt das US-Verfassungsrecht – mit Ausnahme der kalifornischen Verfassung – keine Schutzpflichten. Verfassungsmäßige Rechte wirken ausschließlich im Staat-Bürger-Verhältnis.

– Die Unterschiede lassen sich erklären mit einem grundlegend anderen Verständnis der Rolle des Staates für das Alltagsleben der Bürger. In Deutschland kommt der sozialen Komponente der Marktwirtschaft eine bedeutende Stellung zu.

In der liberalen Tradition der Vereinigten Staaten liegt ein weitaus größerer Schwerpunkt darauf, durch einen freien Markt und ohne unnötige Einmischung des Staates das Leben zu gestalten.

V. Rechtfertigung der Verhinderung der Preisgabe

– Die zu berücksichtigenden verfassungsmäßigen Rechte unterscheiden sich in beiden Verfassungen.

Maßnahmen zur Unterstützung informationellen Selbstschutzes greifen jeweils nicht in die Rechte der Preisgebenden ein. In Deutschland werden erzwungener Schutz und Entscheidungsarchitekturen insbesondere am Recht auf informationelle Selbstbestimmung der Preisgebenden gemessen. In Einzelfällen können auch die Informations-, Meinungs- und Berufsfreiheit einschlägig sein. Unerheblich ist, ob explizite oder implizite Preisgabe verhindert werden soll. In den USA ist die erzwungene Verhinderung expliziter Preisgabe an der Redefreiheit zu messen, während in allen übrigen Fällen nur der prozessuale Due-Process-Schutz gilt.

Alle Maßnahmen sind zusätzlich an den Rechten der verantwortlichen Stellen zu messen. In Deutschland ist in erster Linie die Berufsfreiheit einschlägig, in Ausnahmefällen auch die Eigentumsgarantie, die Meinungsfreiheit und subsidiär die wirtschaftliche Betätigungsfreiheit. In den Vereinigten Staaten ist die nur schwer einschränkbare Redefreiheit betroffen.

– Sollen selbstbestimmt Preisgebende vor sich selbst geschützt werden, dürfen in beiden Rechtsordnungen keine Maßnahmen ergriffen werden, es sei denn, sie dienen gerade der Herstellung oder Erhaltung der Selbstbestimmung. Unter den letztgenannten Umständen darf in Deutschland explizite und implizite Preisgabe verhindert werden, indem informationeller Selbstschutz unterstützt und, soweit erforderlich, Entscheidungsarchitekturen angewandt werden. In den USA darf lediglich versucht werden, die Nutzer durch die Unterstützung informationellen Selbstschutzes und, soweit erforderlich, durch Entscheidungsarchitekturen von impliziter Preisgabe abzuhalten.

– Zum Schutz nicht selbstbestimmt Preisgebender dürfen in beiden Rechtsordnungen alle jeweils notwendigen Maßnahmen ergriffen werden, wobei erzwungener Schutz regelmäßig das einzig wirksame Mittel ist.

– Dienen die Maßnahmen dem Schutz Dritter, können in Deutschland nach Herstellung praktischer Konkordanz mit den Rechten der Preisgebenden Maßnahmen aus allen drei Kategorien gerechtfertigt sein. Dabei können die konkurrierenden Rechte als gleichrangig angesehen werden. Regelmäßig wird erzwungener Schutz das einzig wirksame Mittel sein. In den Vereinigten Staaten lassen sich erzwungener Schutz und Entscheidungsarchitekturen nur dann rechtfertigen, wenn sich die Rechte Dritter tatsächlich gegen die Redefreiheit der Preisgebenden durchsetzen. Aufgrund der herausragenden Bedeutung der Redefreiheit beschränkt sich dies auf

Einzelfälle. Nur die Unterstützung informationellen Selbstschutzes kann problemlos gerechtfertigt werden.

In Deutschland lassen sich zum Schutz abstrakter gesellschaftlicher Belange die Unterstützung informationellen Selbstschutzes sowie, wenn erforderlich, Entscheidungsarchitekturen rechtfertigen, nicht aber erzwungener Schutz. In den Vereinigten Staaten ist zum Schutz abstrakter gesellschaftlicher Belange lediglich die Unterstützung informationellen Selbstschutzes zulässig.

– Die unterschiedlichen Möglichkeiten zur Verhinderung informationeller Preisgabe in Deutschland und den Vereinigten Staaten lassen sich maßgeblich auf drei Unterschiede im Grundrechtsverständnis zurückführen: den in Deutschland höheren Stellenwert der informationellen Privatheit, die große Bedeutung der Redefreiheit der Preisgebenden in den USA sowie die in Deutschland geringere Bedeutung der Rechte der verantwortlichen Stellen.

VI. Ausblick

– Nutzer geben häufig ihre Privatheit in vorhersehbar irrationaler Weise preis. Dem kann theoretisch durch den Einsatz von Entscheidungsarchitekturen entgegengewirkt werden. Insbesondere in den USA besteht die Tendenz, diese auch zum Schutz selbstbestimmt Handelnder einsetzen zu wollen, um irrationales Verhalten zu verhindern.

Das Argument, durch libertären Paternalismus würde nicht etwa Selbstbestimmung genommen, sondern solche ermöglicht, überzeugt allerdings nicht. Auch irrationale Entscheidungen stellen selbstbestimmte Entscheidungen dar. Über diese darf sich der Staat nicht zum Schutz der Handelnden hinwegsetzen.

Die Verhinderung irrationaler Preisgabe stellt nach US-Verfassungsrecht keinen legitimen Eingriffszweck dar. Die US-Rechtsprechungspraxis bleibt jedoch abzuwarten.

Eine Übertragung des Ansatzes, irrationale Preisgabe durch Entscheidungsarchitekturen zu verhindern, auf Deutschland ist, jedenfalls soweit es um den verbindlichen Einsatz von Entscheidungsarchitekturen zum Schutz selbstbestimmt Preisgebender vor sich selbst geht, nicht mit dem Grundgesetz vereinbar.

– Zur Verhinderung rechtspolitisch als gefährlich eingestufter Preisgabe sollte alternativ der Ansatz des partiellen informationellen Selbstschutzes verfolgt werden. Er besitzt Überzeugungskraft sowohl für das deutsche als auch für das US-amerikanische Rechtssystem. Zur Verhinderung informationeller Preisgabe bietet sich ein Vorgehen in drei Schritten an:

Zunächst kann nicht selbstbestimmte informationelle Preisgabe verhindert werden. Im Grenzbereich zwischen Selbstbestimmung und fehlender Selbstbestimmung bietet es sich an, in großzügiger Weise zu typisieren. Zudem besteht eine Befugnis und in Deutschland sogar eine Pflicht, Maßnahmen zur Sicherung der Selbstbestimmung der Preisgebenden zu ergreifen. Neben der Unterstützung infor-

mationellen Selbstschutzes ist es insbesondere in Deutschland zulässig und sachgerecht, verstärkt auf den Einsatz von Entscheidungsarchitekturen zurückzugreifen, um die Selbstbestimmung der Nutzer zu sichern und diese gleichzeitig zu entlasten.

Weiter kann informationelle Preisgabe verhindert werden, wenn sie Allgemeinwohlbelange gefährdet. Häufig löst ein Verhalten gleichzeitig Gefahren für die Preisgebenden und das Allgemeinwohl aus. In beiden Verfassungsordnungen ist es zulässig und angezeigt, Preisgabe primär zum Schutz des Allgemeinwohls zu verhindern und als Nebeneffekt die Preisgebenden vor sich selbst zu schützen. In Deutschland steht dem Gesetzgeber dabei eine weitere Einschätzungsprärogative zu als in den USA.

Schließlich kann informationeller Selbstschutz unterstützt werden. Insbesondere erscheint es sachgerecht, verstärkt mit kartellrechtlichen Mitteln Internetkonzerne am Missbrauch marktbeherrschender Stellungen zu hindern und dadurch die freie Wahl der Nutzer zu schützen. Weiter sollte die Einführung regulierter Selbstregulierungen forciert und ihre Durchsetzung im Wege des Rechts des unlauteren Wettbewerbs erzielt werden. Angesichts der Schnelllebigkeit des Internets und der Vielzahl der damit verbundenen Gefahren und Möglichkeiten wird man auch eine gestärkte Eigenverantwortung der Nutzer akzeptieren und einfordern müssen. Das liberale Verständnis der USA kann hier als Beispiel auch für Deutschland gelten.

– Das weltweite Tätigwerden vieler Internetkonzerne und die rechtlichen, technischen und wirtschaftlichen Verquickungen zwischen Deutschland und den Vereinigten Staaten legen es nahe, durch gemeinsame Forschung einheitliche Standards zur Privatheitswahrung der Nutzer zu setzen. Auch wenn diese voraussichtlich in Deutschland verstärkt auf gesetzlicher Basis umgesetzt werden, während in den USA Selbstverpflichtungen der Unternehmen der Implementierung dienen, wird so faktisch der Privatheitsschutz in beiden Ländern schrittweise angeglichen.

B. Fazit

„Caring about not caring about privacy“[1] – diese eingangs zitierte Forderung hat sich als treffend erwiesen. Angesichts zahlreicher Gefahren informationeller Preisgabe im Internet sollte sowohl dem deutschen als auch dem US-amerikanischen Staat an der informationellen Privatheit seiner Bürger gelegen sein.

Ein nicht zu leugnendes Bedrohungspotenzial geht dabei von den selbstbestimmt Preisgebenden aus. Sollen die mit informationeller Preisgabe verbundenen Gefahren verhindert werden, ist es sachgerecht, den Bürgern in gewissen Situationen auch „Privatheit wider Willen“ aufzuerlegen. Ein solches Vorgehen stellt jedoch in beiden Rechtsordnungen einen Eingriff sowohl hinsichtlich der Nutzerrechte als auch hinsichtlich der Rechte der verantwortlichen Stellen dar. Verfassungsdogmatisch

---

[1] *Allen*, Unpopular Privacy, 2011, 171.

unrichtig und an der tatsächlichen Bedrohungslage vorbeigehend wäre es, informationelle Preisgabe nur um den Schutz der selbstbestimmt Preisgebenden willen zu verhindern. Damit würde den Nutzern vielmehr um ihrer Privatheit und damit Autonomie willen die Autonomie genommen, eigene Entscheidungen zu treffen. Ein solches Vorgehen wäre widersprüchlich.

Daraus folgt nicht, dass informationelle Preisgabe nie staatlicherseits verhindert werden kann. Doch bedarf es einer feinen Ausdifferenzierung und der Heranziehung von Rechtfertigungsgründen, die über den Schutz der selbstbestimmt Handelnden vor sich selbst hinausgehen. Neben der Zivilgesellschaft ist auch der Staat zur Lenkung informationeller Preisgabe aufgerufen und zwar in einer Weise, die den drohenden Gefahren Rechnung trägt, ohne das Selbstbestimmungsrecht der Einzelnen und die Rechte der verantwortlichen Stellen unverhältnismäßig zu beeinträchtigen. Die selbstbestimmte Entscheidung der Nutzer zur Aufgabe der Privatheit muss respektiert werden und es muss zudem Spielraum für auf Datenverarbeitung beruhenden technischen Fortschritt verbleiben. Hierfür bietet sich das Konzept des partiellen informationellen Selbstschutzes an. Dieser ermöglicht die Verhinderung von Preisgabe immer dann, wenn von ihr besonders gravierende Bedrohungen ausgehen. In allen anderen Fällen bedarf es keines Schutzes. Der freiheitlich-demokratische Staat muss vielmehr ein Grundvertrauen darein haben, dass selbstbestimmt handelnde Bürger ihre Freiheiten ohne staatliche Hilfe eigenverantwortlich nutzen können.

English Abstract

Coercing Online Privacy[1]

In today's society, competent adult internet users voluntarily disclose vast amounts of personal data. This can have numerous advantages, such as economic benefits and greater convenience. Nevertheless such voluntary disclosure can cause great harm to individuals.

Governments may feel that through minor interventions they can protect their citizens from disclosure that is not in the latters best interest. Taking a paternalistic role, governments can balance the pros and cons of certain forms of disclosure and prevent disclosure when disadvantages exceed advantages for users. However, must they do so? May they do so? And, if they don't, are they left with their hands tied?

In order to investigate these questions, the current study compares the approach taken by the government of Germany, one of the most influential jurisdictions within the European Union, with that of the United States, where the headquarters of the leading online businesses are located.

The study focuses on online privacy, understood as informational privacy in the internet environment. Informational privacy entails the right to decide about the disclosure and use of personal data online. Online privacy can be affected by both explicit and implicit disclosure.

When disclosing data, users are often unaware of the full consequences of doing so. However, as long as they are capable of understanding their decision (unlike, for example, minors and mentally ill people) and do not find themselves in circumstances where their freedom of choice is severely restricted, their disclosure is to be considered voluntary.

In terms of the harms that online disclosure can cause not only to individuals themselves, but also to other individuals and to societal progress and the democratic system as a whole, German and US lawmakers are faced with an identical situation. In both jurisdictions, the endangered interests are afforded constitutional protection, albeit with differences as regards the approach taken.

To protect their citizens from these harms, governments can choose whether to prevent disclosure by enforcing privacy protection, by supporting privacy self-management, or by nudging users into disclosing less.

---

[1] The title pays tribute to: *Allen*, Coercing Privacy, 40 William and Mary L. Rev. (1999), 723 ff.

All of these actions can infringe upon the rights of users and of data collectors, and are only licit when justified by constitutional principles. The users' rights that are affected by government intervention are, in Germany, primarily the right to informational self-determination (Recht auf informationelle Selbstbestimmung), and in the US, the freedom of speech as well as the procedural due process guarantees. The rights of data collectors are, in Germany, above all the freedom of profession (Berufsfreiheit), and, in the United States, the freedom of speech. In the US, the commercial speech rights of data collectors create a particular barrier to all government measures that prevent online disclosure.

If government interventions are aimed at encouraging autonomy, preventing non-autonomous disclosure, protecting the informational privacy of others or supporting social progress and democracy, then they can, under certain circumstances, be justified. In Germany, there may even be a duty to protect most of these values (Schutzpflicht).

However, neither the German nor the US government has the duty or the power to coerce the privacy choices of competent adult users for the sole purpose of protecting them against dangers caused by themselves.

These findings also apply to the use of so-called nudges to correct irrational behavior, a policy discussed particularly in current US scholarship. Preventing irrational disclosure (without aiming at other goals) should not serve as a justification for protecting competent adult users from voluntary disclosure. Individuals regularly make decisions which are not in their best interest and they have a right to do so. Even if the goal of protecting users from making irrational disclosures is a laudable one, doing so would disrespect their free choice. Even if nudges do not coerce users, they de facto force them to consider governments' ideas of how they should live their lives. Users' autonomy entails their right to make their own decisions regarding personal information, even if they are unfavorable or will be regretted later. Hence nudging users into making rational choices is illicit.

In the following, it is suggested that governments should pursue a three-step-approach preventing users from excessive disclosure of information online:

- preventing involuntary online disclosure;
- preventing online disclosure that also harms other interests;
- promoting privacy self-management.

Preventing certain kinds of online disclosure would require that governments in Europe and the United States agree on common privacy protection standards, regardless of whether these standards are enforced via regulation or via government-monitored private sector agreements. In Germany and/or the European Union, standards would likely be enforced by legislation, while in the United States they would largely be left to self-regulation. Despite these different approaches regarding implementation, there is hope that a consensus could be reached on the instruments through which to protect individuals.

Literaturverzeichnis

Alle Webseiten wurden letztmalig im Juni 2015 geprüft. US-amerikanische Rechtsprechung und Literatur werden nach der dort üblichen Zitierweise zitiert.

Abernathy, Charles F., Law in the United States, St. Paul 2006.

Acquisti, Alessandro, Privacy in Electronic Commerce and the Economics of Immediate Gratification, in: Breese, Jack (Hrsg.), Proceedings of the 5th ACM Conference on Electronic Commerce, New York 2004, 21–29.

–, Nudging Privacy. The Behavioral Economics of Personal Information, 6 IEEE Security & Privacy Economics (2009), 82–85.

Acquisti, Alessandro/Gross, Ralph, Imagined Communities: Awareness, Information Sharing, and Privacy on the Facebook, 2006, http://www.heinz.cmu.edu/~acquisti/papers/acquisti-gross-facebook-privacy-PET-final.pdf.

Acquisti, Alessandro/Grossklags, Jens, Privacy and Rationality in Individual Decision Making. Economics of Information Security, 2005, http://csis.pace.edu/~ctappert/dps/d861-09/team2-3.pdf.

–/–, Uncertainty, Ambiguity and Privacy, 6.3.2005, http://www.infosecon.net/workshop/pdf/64.pdf.

–/–, What Can Behavioral Economics Teach us about Privacy?, in: Acquisti, Alessandro/Gritzalis, Stefanos/Lambrinoudakis, Costos/De Capitani di Vimercati, Sabrina (Hrsg.), Digital privacy – Theory, technologies and practices, Boca Raton 2008, 363–377.

Albers, Marion, Grundrechtsschutz der Privatheit, DVBl. 2010, 1061–1069.

Alexy, Robert, Theorie der Grundrechte, Baden-Baden 1985.

Allen, Anita L., Coercing Privacy, 40 William and Mary L. Rev. (1999), 723–757.

–, Dredging up the Past: Lifelogging, Memory, and Surveillance, 75 Chicago L. Rev. (2008), 47–74.

–, Privacy Law and Society, 2. Aufl., St. Paul 2011.

–, Unpopular Privacy: What Must We Hide?, New York 2011.

–, An Ethical Duty to Protect One's Own Informational Privacy?, 64 Alabama L. Rev. (2013), 845–866.

–, Our Privacy Rights and Responsibilities. Replies to Critics, 13 Philosophy and Law (2013), 19–27.

Almunia, Joaquín, Competition and personal data protection, Brüssel 26.11.2012, http://europa.eu/rapid/press-release_SPEECH-12-860_en.htm.

Amelung, Ulrich, Der Schutz der Privatheit im Zivilrecht. Schadensersatz und Gewinnabschöpfung bei Verletzung des Rechts auf Selbstbestimmung über personenbezogene Informationen im deutschen, englischen und US-amerikanischen Recht, Tübingen 2002.

Arendt, Hannah, Vita Activa. oder vom tätigen Leben, 2. Aufl., Zürich/München 2003.

Ariely, Dan, Predictably irrational. The hidden forces that shape our decisions, 2. Aufl., New York 2010.

Augsburger, Matthias, Lauterkeitsrechtliche Beurteilung von Corporate Responsibility Codes. Verbindliche Standards im Wettbewerb?, MMR 2014, 427–431.

Ausloss, Jef, The 'Right to be Forgotten'. Worth remembering?, 28 Computer Law & Security Review (2012), 143–152.

Baehr, Robert J., A New Wave of Paternalistic Tobacco Regulation, 95 Iowa L. Rev. (2010), 1663–1696.

Bakos, Yannis/Marotta-Wurgler, Florencia/Trossen, David R., Does Anyone Read the Fine Print? Testing a Law and Economics Approach to Standard Form Contracts, Law & Economics Research Paper Series, 10.2009.

Balkin, Jack M., Living originalism, Cambridge, Mass. 2011.

Bamberger, Heinz Georg/Roth, Herbert (Hrsg.), Beck'scher Online-Kommentar BGB, 35. Aufl., München 1.5.2015 (zit. Beck-OK BGB/*Bearbeiter*).

Bamberger, Kenneth A./Mulligan, Deirdre K., Privacy on the Books and on the Ground, 63 Stanford L. Rev. Online (2011), 247–316.

Barakat, Matthew, Scalia Expects NSA Program to End Up in Court, 25.9.2013, http://bigstory.ap.org/article/scalia-expects-nsa-wiretaps-end-court.

Bauer, Jobst-Hubertus/Günther, Jens, Kündigung wegen beleidigender Äußerungen auf Facebook. Vertrauliche Kommunikation unter Freunden?, NZA 2013, 67–73.

Baum, Gerhart R., Unerledigte Verfassungsaufträge, DuD 2011, 595–597.

Baumann, Bastian, Grenzüberschreitender Datenaustausch: Passagierdaten und Passagierrechte, in: Dix, Alexander/Franßen, Gregor/Kloepfer, Michael/Schaar, Peter/Schoch, Friedrich/Voßhoff, Andrea/Deutsche Gesellschaft für Informationsfreiheit (Hrsg.), Informationsfreiheit und Informationsrecht – Jahrbuch 2014, Berlin 2015, 29–64.

Bensberg, Frank, Die technischen Potenziale analytischer Informationssysteme – eine Grundlage für den interdisziplinären Dialog, in: Redeker, Helmut/Hoppen, Peter (Hrsg.), DGRI Jahrbuch 2011, Köln 2012, 181–200.

Bentham, Jeremy, Panoptikum oder Das Kontrollhaus. Aus dem Englischen von Andreas Leopold Hofbauer, Berlin 2013 (Original: 1791).

Berger, Karola/Kraska, Sebastian, Datenschutz im Web 2.0: Wann gilt das deutsche Bundesdatenschutzgesetz?, 2012, http://www.iitr.de/datenschutz-im-web-2-0-wann-gilt-das-deutsche-bundesdatenschutzgesetz.html.

Berliner Beauftragter für Datenschutz und Informationsfreiheit, Bericht 2011, Berlin 2011.

Bernert-Auerbach, Ulrike, Das Recht auf den eigenen Tod und aktive Sterbehilfe unter verfassungsrechtlichen Gesichtspunkten, Frankfurt am Main 2012.

Bethge, Herbert, Grundpflichten als verfassungsrechtliche Dimension, NJW 1982, 2145–2150.

Beuth, Patrick, Datensammelwut als Spiel, 28.3.2012, http://www.zeit.de/digital/games/2012-03/spiel-data-dealer/.

Beyvers, Eva/Herbrich, Tilman, Das Niederlassungsprinzip im Datenschutzrecht – am Beispiel von Facebook. Der neue Ansatz des EuGH und die Rechtsfolgen, ZD 2014, 558–562.

Böckenförde, Ernst-Wolfgang, Demokratie als Verfassungsprinzip, in: Isensee, Josef/Kirchhof, Paul (Hrsg.), Handbuch des Staatsrechts der Bundesrepublik Deutschland II – Verfassungsstaat, 3. Aufl., Heidelberg 2004, 429–496.

Bothun, Deborah/Lieberman, Matt/Tipton, Gretchen, Consumer privacy: What are consumers willing to share?, 2012, http://www.pwc.com/us/en/industry/entertainment-media/publications/consumer-intelligence-series/consumer-privacy.jhtml.

Bracha, Oren/Pasquale, Frank, Federal Search Commission? Access, Fairness and Acountability in the Law of Search, 93 Cornell L. Rev. (2008), 1149–1209.

Bräutigam, Peter, Das Nutzungsverhältnis bei sozialen Netzwerken. Zivilrechtlicher Austausch von IT-Leistung gegen personenbezogene Daten, MMR 2012, 635–641.

Britz, Gabriele, Einzelfallgerechtigkeit versus Generalisierung. Verfassungsrechtliche Grenzen statistischer Diskriminierung, Tübingen 2008.

–, Europäisierung des grundrechtlichen Datenschutzes?, EuGRZ 2009, 1–11.

–, Informationelle Selbstbestimmung zwischen rechtswissenschaftlicher Grundsatzkritik und Beharren des Bundesverfassungsgerichts, in: Hoffmann-Riem, Wolfgang (Hrsg.), Offene Rechtswissenschaft – Ausgewählte Schriften von Wolfgang Hoffmann-Riem und begleitende Analysen, Tübingen 2010, 561–596.

Bronwlee, John, GameStation EULA collects 7,500 souls from unsuspecting customers, 16.4.2010, http://www.geek.com/games/gamestation-eula-collects-7500-souls-from-unsuspecting-customers-1194091/.

Brugger, Winfried, Grundrechte und Verfassungsgerichtsbarkeit in den Vereinigten Staaten von Amerika, Tübingen 1987.

–, Angloamerikanischer Einfluss auf die Grundrechtsentwicklung in Deutschland, in: Isensee, Josef/Kirchhof, Paul (Hrsg.), Handbuch des Staatsrechts der Bundesrepublik Deutschland X, 3. Aufl., Heidelberg 2011, 121–152.

Brüning, Christoph, Voraussetzungen und Inhalt eines grundrechtlichen Schutzanspruchs. Anmerkung zu BVerwG, NVwZ 1999, 1234, JuS 2000, 955–959.

Buchner, Benedikt, Informationelle Selbstbestimmung im Privatrecht, Tübingen 2006.

–, Eigentumsrechte an persönlichen Daten?, in: Redeker, Helmut/Hoppen, Peter (Hrsg.), DGRI Jahrbuch 2011, Köln 2012, 53–63.

Bull, Hans Peter, Zweifelsfragen um die informationelle Selbstbestimmung – Datenschutz als Datenaskese?, NJW 2006, 1617–1624.

–, Informationelle Selbstbestimmung – Vision oder Illusion?, Tübingen 2009.

–, Persönlichkeitsschutz im Internet: Reformeifer mit neuen Ansätzen, NVwZ 2011, 257–263.

–, Netzpolitik: Freiheit und Rechtsschutz im Internet, Baden-Baden 2013.

Bundesministerium der Justiz und für Verbraucherschutz, Mailen, Surfen, Chatten – Wie ist die Privatsphäre zu retten? Konferenz von BMJV und BITKOM am „Safer Internet Day" diskutiert Fragen zur Sicherheit der digitalen Kommunikation, Berlin 11.2.2014, http://www.bmjv.de/SharedDocs/Pressemitteilungen/DE/2014/20140211_Safer_Internet_Day.html;jsessionid=C38715A4763AFB4AF4D4C8B29F3227F3.1_cid289?nn=1468684.

Bundesministerium des Innern, Ideenwettbewerb „Vergessen im Internet". Bundesinnenminister Dr. Hans-Peter Friedrich zeichnet die kreativsten Beiträge aus, 7.5.2012, http://www.bmi.bund.de/SharedDocs/Pressemitteilungen/DE/2012/05/acatech.html.

Bundesverband Informationswirtschaft, Telekommunikation und neue Medien e.V., Vor zehn Jahren wurde Facebook gegründet, Berlin 31.1.2014, http://www.bitkom.org/de/markt_statistik/64018_78533.aspx.

Bunge, Felix, Über die kollektive Schutzrichtung des Rechts auf informationelle Selbstbestimmung, ZD-Aktuell 2015, 04635.

Calliess, Christian, Schutzpflichten, in: Merten, Detlef/Papier, Hans-Jürgen (Hrsg.), Handbuch der Grundrechte in Deutschland und Europa II – Grundrechte in Deutschland: Allgemeine Lehren I, Heidelberg 2006, 963–992.

Calliess, Christian/Ruffert, Matthias (Hrsg.), EUV, AEUV. Das Verfassungsrecht der Europäischen Union mit Europäischer Grundrechtecharta, 4. Aufl., München 2011.

Calo, Ryan M., Against Notice Skepticism in Privacy (and Elsewhere), 87 Notre Dame L. Rev. (2012), 1027–1072.

–, Code, Nudge, or Notice? University of Washington School of Law Legal Studies Research Paper, 4.2013, http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2217013.
Camerer, Colin/Issacharoff, Samuel/Loewenstein, George/O'Donoghue, Ted/Rabin, Matthew, Regulation for Conservatives: Behavioral Economics and the Case of "Asymmetric Paternalism", 151 Univ. of Pennsylvania L. Rev. (2003), 1211–1254.
Canaris, Claus-Wilhelm, Grundrechte und Privatrecht, 184 AcP (1984), 201–246.
–, Grundrechtswirkungen und Verhältnismäßigkeitsprinzip in der richterlichen Anwendung und Fortbildung des Privatrechts, JuS 1989, 161–172.
Chandler, Jennifer A., A Right to Reach an Audience: An Approach to Intermediary Bias on the Internet, 35 Hofstra L. Rev. (2007), 1095–1137.
Clarke, Roger, Information Technology and Dataveillance, 11.1987, http://www.rogerclarke.com/DV/CACM88.html.
Cohen, Jean L., Regulating Intimacy. A New Legal Paradigm, Princeton/Oxford 2002.
Cohen, Julie E., Examined Lives: Informational Privacy and the Subject as Object, 52 Stanford L. Rev. Online (2000), 1373–1438.
–, DRM and Privacy, 18 Berkeley Tech. L. J. (2003), 575–617.
–, What Privacy is For, 126 Harvard L. Rev. (2013), 1904–1933.
Constantinesco, Leóntin-Jean, Rechtsvergleichung. Einführung in die Rechtsvergleichung, Köln/Berlin/Bonn/München 1971.
Cooter, Robert/Ulen, Thomas, Law & Economics, 6. Aufl., Boston 2010.
Cremer, Wolfgang, Die Verhältnismäßigkeitsprüfung bei der grundrechtlichen Schutzpflicht. Abwägung von Grund und Gegengrund statt Gewährleistung eines angemessen Schutzniveaus, DÖV 2008, 102–108.
DANA Redaktion, NSA scannt Netz nach Gesichtern, DANA 2014, 122.
Danckert, Burkhard/Mayer, Frank Joachim, Die vorherrschende Meinungsmacht von Google. Bedrohung durch einen Informationsmonopolisten?, MMR 2010, 219–222.
Danezis, George/Domingo-Ferrer, Josep/Hansen, Marit/Hoepman, Jaap-Henk/Le Métayer, Daniel/Tirtea, Rodica/Schiffner, Stefan, Privacy and Data Protection by Design – from policy to engineering, Brüssel 12.2014.
Das, Sauvik/Kramer, Adam, Self-Censorship on Facebook, in: Kiciman, Emre/Ellison, Nicole B./Hogan, Bernie/Resnick, Paul/Soboroff, Ian (Hrsg.), Proceedings of the Seventh International AAAI Conference on Weblogs and Social Media – 8–11 July 2013, Palo Alto 2013, 120–127.
Dehmel, Susanne, Selbstregulierung – das Selbstregulierungsabkommen für soziale Netzwerke und generelle Überlegungen, in: Hill, Hermann/Martini, Mario/Wagner, Edgar (Hrsg.), Facebook, Google & Co. – Chancen und Risiken, Baden-Baden 2013, 135–141.
Der Spiegel, Kampf den Avataren. Google missbraucht seine Macht und muss daher von der Politik neue Regeln bekommen, Der Spiegel 21/2014, 12.
–, „Wir sind keine Labormäuse", Der Spiegel 15/2015, 38–39.
Deutscher Juristentag, Beschlüsse des 69. Deutschen Juristentags, Bonn 2012.
Diesterhöft, Martin, Das Recht auf digitalen Neubeginn. Die „Unfähigkeit des Internets zu vergessen" als Herausforderung für das allgemeine Persönlichkeitsrecht, Berlin 2014.
Dietlein, Johannes, Die Lehre von den grundrechtlichen Schutzpflichten, Berlin 1992.
Diggelmann, Oliver, Grundrechtsschutz der Privatheit, in: Höfling, Wolfram (Hrsg.), Der Schutzauftrag des Rechts – Referate und Diskussionen auf der Tagung der Vereinigung der Deutschen Staatsrechtslehrer in Berlin vom 29. September bis 2. Oktober 2010, Berlin 2011, 50–81.

Doehring, Karl, Die Gesunderhaltung des Menschen im Spannungsverhältnis zwischen Staatsfürsorge und Individualentscheidung, in: Fürst, Walther/Herzog, Roman/Umbach, Dieter C. (Hrsg.), Festschrift für Wolfgang Zeidler Band II, Berlin, New York 1987, 1553–1565.

Dörr, Dieter/Natt, Alexander, Suchmaschinen und Meinungsvielfalt. Ein Beitrag zum Einfluss von Suchmaschinen auf die demokratische Willensbildung, ZUM 2014, 829–847.

Douglas, Jack D., Cooperative Paternalism versus Conflictful Paternalism, in: Sartorius, Ralf (Hrsg.), Paternalism, Minneapolis 1983, 171–200.

Downs, Anthony, An Economic Theory of Political Action in a Democracy, 65 J. of Political Economy (1957), 135–150.

Dreier, Horst, (Hrsg.), Grundgesetz-Kommentar I. Präambel, Artikel 1–19, 3. Aufl., Tübingen 2013.

Dröge, Cordula, Positive Verpflichtungen der Staaten in der Europäischen Menschenrechtskonvention, Berlin, Heidelberg, New York 2003.

Duhigg, Charles, How Companies Learn Your Secrets, 16.02.2012, http://www.nytimes.com/2012/02/19/magazine/shopping-habits.html?pagewanted=1&_r=2&hp&.

Dürig, Günter, Grundrechte und Privatrechtsprechung, in: Maunz, Theodor (Hrsg.), Vom Bonner Grundgesetz zur gesamtdeutschen Verfassung – Festschrift zum 75. Geburtstag von Hans Nawiasky, München 1956, 157–190.

Dürrenmatt, Friedrich, Die Panne. Ein Hörspiel und eine Komödie, Zürich 1985 (Original: 1961).

Dwork, Cynthia/Mulligan, Deirdre K., It's Not Privacy, And It's Not Fair, 66 Stanford L. Rev. Online (2013), 35–40.

Dworkin, Gerald, Paternalism, in: Sartorius, Ralf (Hrsg.), Paternalism, Minneapolis 1983, 19–34.

Eidenmüller, Horst, Effizienz als Rechtsprinzip. Möglichkeiten und Grenzen der ökonomischen Analyse des Rechts, Tübingen 1995.

–, Liberaler Paternalismus, JZ 2011, 814–821.

Elkin-Koren, Niva, Let the Crawlers Crawl: On Virtual Gatekeepers and the Right to Exclude Indexing, 76 Dayton L. Rev. (2001), 179–209.

Englerth, Markus, Behavioral Law and Economics – eine kritische Einführung, in: Engel, Christoph/Englerth, Markus/Lüdemann, Jörn/Spiecker genannt Döhmann, Indra (Hrsg.), Recht und Verhalten – Beiträge zu Behavioral Law and Economics, Tübingen 2007, 60–130.

–, Vom Wert des Rauchens und der Rückkehr der Idioten – Paternalismus als Antwort auf beschränkte Rationalität?, in: Engel, Christoph/Englerth, Markus/Lüdemann, Jörn/Spiecker genannt Döhmann, Indra (Hrsg.), Recht und Verhalten – Beiträge zu Behavioral Law and Economics, Tübingen 2007, 231–258.

Epping, Volker/Hillgruber, Christian (Hrsg.), Beck'scher Online-Kommentar GG, 24. Aufl., München 1.3.2015 (zit. Beck-OK GG/*Bearbeiter*).

Erichsen, Hans-Uwe, Grundrechtliche Schutzpflichten in der Rechtsprechung des Bundesverfassungsgerichts, JURA 1997, 85–89.

Europäische Kommission, Special Eurobarometer 359. Attitudes on Data Protection and Electronic Identity in the European Union, Brüssel 6.2011, http://ec.europa.eu/public_opinion/archives/ebs/ebs_359_en.pdf.

–, Kartellrecht: Kommission übermittelt Google Mitteilung der Beschwerdepunkte zu seinem Preisvergleichsdienst und leitet außerdem förmliche Untersuchung zu Android ein, Brüssel 15.4.2015, http://europa.eu/rapid/press-release_IP-15-4780_de.htm.

Europäischer Datenschutzbeauftragter, Stellungnahme. des Europäischen Datenschutzbeauftragten zur Mitteilung der Kommission an das Europäische Parlament, den Rat, den Europäischen Wirtschafts- und Sozialausschuss und den Ausschuss der Regionen – „Europäische Strategie für ein besseres Internet für Kinder“, Brüssel 17.7.2012, http://www.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Opinions/2012/12-07-17_Better_Iternet_Children_DE.pdf.

Ewer, Wolfgang/Thienel, Tobias, Völker-, unions- und verfassungsrechtliche Aspekte des NSA-Datenskandals, NJW 2014, 30–36.

Fateh-Moghadam, Bijan, Die Einwilligung in die Lebendorganspende. Die Entfaltung des Paternalismusproblems im Horizont differenter Rechtsordnungen am Beispiel Deutschlands und Englands, München 2008.

–, Grenzen des weichen Paternalismus. Blinde Flecken der liberalen Paternalismuskritik, in: Fateh-Moghadam, Bijan/Sellmaier, Stephan/Vossenkuhl, Wilhelm (Hrsg.), Grenzen des Paternalismus, Stuttgart 2010, 21–47.

FDR Group, The Impact of US Government Surveillance on Writers. Findings from a Survey of PEN Membership. Conducted for the PEN American Center, 31.10.2013, http://www.pen.org/sites/default/files/Chilling%20Effects_PEN%20American.pdf.

Federal Trade Commission, FTC Strengthens Kids’ Privacy, Gives Parents Greater Control Over Their Information By Amending Children’s Online Privacy Protection Rule, 19.12.2012, http://www.ftc.gov/opa/2012/12/coppa.shtm.

Federath, Hannes/Pfitzmann, Andreas, Technische Grundlagen, in: Roßnagel, Alexander (Hrsg.), Handbuch Datenschutzrecht – Die neuen Grundlagen für Wirtschaft und Verwaltung, München 2003, 61–84.

Feinberg, Joel, Legal Paternalism, in: Sartorius, Ralf (Hrsg.), Paternalism, Minneapolis 1983, 3–18.

Fenchel, Jörg, Negative Informationsfreiheit. Zugleich ein Beitrag zur negativen Grundrechtsfreiheit, Berlin 1997.

Ferony, Peter, Constitutional Law – From Goblins to Graveyards: The Problem of Paternalism in Compelled Perception, 35 Western New England L. Rev. (2013), 205–248.

Feuz, Martin/Fuller, Matthew/Stalder, Felix, Personal Web Searching in the Age of Semantic Capitalism: Diagnosing the Mechanisms of Personalization, 16 First Monday (2011).

Fisahn, Andreas, Ein unveräußerliches Grundrecht am eigenen genetischen Code, ZRP 2001, 49–54.

Fischer, Kai, Die Zulässigkeit aufgedrängten staatlichen Schutzes vor Selbstschädigung, Frankfurt am Main 1997.

Fischhoff, Baruch, Debiasing, in: Kahneman, Daniel/Slovic, Paul/Tversky, Amos (Hrsg.), Judgement under uncertainty: Heuristics and biases, Cambridge 1982, 422–444.

Fischinger, Philipp S., Der Grundrechtsverzicht, JuS 2007, 808–813.

Foucault, Michel, Überwachen und Strafen. Die Geburt des Gefängnisses, Frankfurt am Main 1976.

Frohmann, Larry, Only Sheep Let Themselves Be Counted. Privacy, Political Culture, and the 1983/87 West German Census Boycotts, in: Friedrich-Ebert-Stiftung (Hrsg.), Archiv für Sozialgeschichte, Bonn 2012, 335–378.

Fuchs, Christian/Goetz, John, Geheimer Krieg. Wie von Deutschland aus der Kampf gegen den Terror gesteuert wird, Reinbek bei Hamburg 2013.

Gardbaum, Stephen, The Myth and the Reality of American Constitutional Exceptionalism, 107 Mich. L. Rev. (2009), 391–466.

Gavison, Ruth, Privacy and the Limits of Law, 89 Yale L. J. (1980), 421–471.

Genz, Alexander, Datenschutz in Europa und den USA. Eine rechtsvergleichende Untersuchung unter besonderer Berücksichtigung der Safe-Harbor-Lösung, Wiesbaden 2004.

Geuss, Raymond, Privatheit. Eine Genealogie, Frankfurt am Main 2002.

GfK Verein, Deutsche fürchten Datenmissbrauch, Nürnberg 12.11.2013, http://www.gfk.com/de/news-und-events/presse/pressemitteilungen/seiten/deutsche-fuerchten-datenmissbrauch.aspx.

–, Maßnahmen der Internetnutzer: Digitaler Selbstschutz und Verzicht, Nürnberg 21.11.2013, http://www.gfk.com/de/news-und-events/presse/pressemitteilungen/seiten/ma%C3%9Fnahmen-der-internetnutzer-digitaler-selbstschutz-und-verzicht.aspx.

Giegerich, Thomas, Privatwirkung der Grundrechte in den USA. Die State Action Doctrine des U.S. Supreme Courts und die Bürgerrechtsgesetzgebung des Bundes, Berlin/Heidelberg/New York 1992.

Gimmler, Roland, Medienkompetenz und Datenschutzkompetenz in der Schule, DuD 2012, 110–116.

Globig, Klaus, Zulässigkeit der Erhebung, Verarbeitung und Nutzung im öffentlichen Bereich, in: Roßnagel, Alexander (Hrsg.), Handbuch Datenschutzrecht – Die neuen Grundlagen für Wirtschaft und Verwaltung, München 2003, 627–677.

Gola, Peter/Klug, Christoph/Körffer, Barbara/Schomerus, Rudolf (Hrsg.), Bundesdatenschutzgesetz, 12. Aufl., München 2015 (zit. Gola/Schomerus-BDSG/*Bearbeiter*).

Gramm, Christof, Rechtsfragen der staatlichen AIDS-Aufklärung, NJW 1989, 2917–2926.

Graßhof, Karin, The Duty to Protect and to Ensure Human Rights and the Basic Law of the Federal Republic of Germany, in: Klein, Eckart (Hrsg.), The Duty to Protect and to Ensure Human Rights – Colloquium Potsdam, 1–3 July 1999, Berlin 2000, 33–51.

Greve, Holger, Internetregulierung zwischen Grundrechtsermöglichung und Informationsrestriktion, DAJV Newsletter 2013, 164–169.

Grimm, Rüdiger, Spuren im Netz, DuD 2012, 88–91.

Grimmelmann, James, Saving Facebook, 94 Iowa L. Rev. (2009), 1137–1206.

Gurlit, Elke, Verfassungsrechtliche Rahmenbedingungen des Datenschutzes, NJW 2010, 1035–1041.

Gusy, Christoph, Rechtsgüterschutz als Staatsaufgabe. Verfassungsfragen der „Staatsaufgabe Sicherheit“, DÖV 1996, 573–583.

Gutmann, Thomas, Gesetzgeberischer Paternalismus ohne Grenzen? Zum Beschluß des Bundesverfassungsgerichts zur Lebendspende von Organen, NJW 1999, 3387–3389.

Gutwald, Rebecca, Autonomie, Rationalität und Perfektionismus. Probleme des weichen Paternalismus im Rechtfertigungsmodell der Bounded Rationality, in: Fateh-Moghadam, Bijan/Sellmaier, Stephan/Vossenkuhl, Wilhelm (Hrsg.), Grenzen des Paternalismus, Stuttgart 2010, 73–93.

Häberle, Peter, Die Wesensgehaltgarantie des Artikel 19 Abs. 2 Grundgesetz. Zugleich ein Beitrag zum institutionellen Verständnis der Grundrechte und zur Lehre vom Gesetzesvorbehalt, 3. Aufl., Heidelberg 1983.

Hain, Karl-Eberhard, Der Gesetzgeber in der Klemme zwischen Übermaß- und Untermaßverbot?, DVBl. 1993, 982–984.

Hamann, Götz/Rohwetter, Marcus, Vier Sheriffs zensieren die Welt. Wie Apple, Facebook, Amazon und Google dem Internet ihre Gesetze aufzwingen, 2.8.2012, http://www.zeit.de/2012/32/Zensur-Apple-Facebook-Amazon-Google/.

Hamann, Hanjo/Hermstrüwer, Yoan, Biometrie und Behavioral Economics. Verhaltensökonomische Perspektiven auf das europäische Datenschutzrecht, KJ 2013, 184–197.

Hamburger, Ellis, Facebook tests Snapchat-like expiration dates for your posts, 10.9.2014, http://www.theverge.com/2014/9/10/6132699/facebook-testing-snapchat-like-ephemeral-posts-that-disappear.

Hansen, Marit, Privacy Enhancing Technologies, in: Roßnagel, Alexander (Hrsg.), Handbuch Datenschutzrecht – Die neuen Grundlagen für Wirtschaft und Verwaltung, München 2003, 291–324.

–, Überwachungstechnologie, in: Schmidt, Jan-Hinrik/Weichert, Thilo (Hrsg.), Datenschutz – Grundlagen, Entwicklungen und Kontroversen, Bonn 2012, 78–87.

–, Herausforderungen für den selbstbestimmten Bürger, in: Kompetenzzentrum Öffentliche IT (Hrsg.), Menschen in der digitalen Gesellschaft, Berlin 2014, 12–13.

Hansen, Marit/Weichert, Thilo, The Right to Privacy. übersetzt und mit Zwischenüberschriften versehen, https://www.datenschutzzentrum.de/allgemein/20111219-Warren-Brandeis-Recht-auf-Privatheit.html.

Harte-Bavendamm, Henning/Henning-Bodewig, Frauke (Hrsg.), Gesetz gegen den Unlauteren Wettbewerb. Kommentar. Mit Preisgabenverordnung, 3. Aufl., München 2013.

Hartzog, Woodrow/Selinger, Evan, Obscurity: A Better Way to Think About Your Data Than 'Privacy', 17.1.2013, http://www.theatlantic.com/technology/archive/2013/01/obscurity-a-better-way-to-think-about-your-data-than-privacy/267283/.

Hasher, Lynn/Goldstein, David/Toppino, Thomas, Frequency and the Conference of Referencial Validity, 16 J. of Verbal Learning and Verbal Behaviour (1977), 107–112.

Heckmann, Dirk, Öffentliche Privatheit – Der Schutz des Schwächeren im Internet, K&R 2010, 770–777.

–, Digitales Dilemma. Das Recht des Schwächeren im Internet, 2012, http://www.lto.de/recht/hintergruende/h/digitales-dilemma-das-recht-der-schwaecheren-im-internet/.

–, Persönlichkeitsschutz im Internet. Anonymität der IT-Nutzung und permanente Datenverknüpfung als Herausforderungen für Ehrschutz und Profilschutz, NJW 2012, 2631–2635.

Heinig, Hans Michael, Paternalismus im Sozialstaat. Nutzen und Grenzen des Paternalismusdiskurses für eine Verfassungstheorie des Sozialstaates, in: Anderheiden, Michael/Bürkli, Peter/Heinig, Hans Michael/Kirste, Stephan/Seelmann, Kurt (Hrsg.), Paternalismus und Recht – In memoriam Angela Augustin (1968–2004), Tübingen 2006, 157–188.

Heller, Christian, Post-Privacy. Prima leben ohne Privatsphäre, München 2011.

Hermes, Georg, Das Grundrecht auf Schutz von Leben und Gesundheit. Schutzpflicht und Schutzanspruch aus Art. 2 Abs. 2 Satz 1 GG, Heidelberg 1987.

Hermstrüwer, Yoan/Hamann, Hanjo, Biometrie und Autonomie – Die Vermessung der Person zwischen Datenschutzrecht und Entscheidungsforschung, in: Hermstrüwer, Yoan/Hamann, Hanjo/Diers, Rahel M. K. (Hrsg.), Schwimmen mit Fingerabdruck? – Die biometrischen Herausforderungen für das Recht der Gegenwart und Zukunft, Göttingen 2012, 1–44.

Hert, Paul de/Papakonstantinou, Vagelis, The proposed data protection Regulation replacing Directive 95/46/EC. A sound system for the protection of individuals, 28 Computer Law & Security Review (2012), 130–142.

Hill, Claire A., Anti-Anti-Anti Paternalism, 2 New York J. of L. and Liberty (2007), 444–454.

Hillgruber, Christian, Der Schutz des Menschen vor sich selbst, München 1992.

Hinrichs, Ulrike, „Big Brother" und die Menschenwürde, NJW 2000, 2173–2176.

Hobbes, Thomas, Leviathan. Edited with an Introduction by C. B. Macpherson, Harmondsworth, Middlesex 1982 (Original: 1651).

Hoeren, Thomas/Sieber, Ulrich/Holznagel, Bernd (Hrsg.), Handbuch Multimedia-Recht. Rechtsfragen des elektronischen Geschäftsverkehrs, 41. EL., München 3.2015.

Hoffmann, Catherine, Politik per Psychotrick. Verhaltensforschung am Bürger, 11.3.2015, http://www.sueddeutsche.de/wirtschaft/verhaltensforschung-am-buerger-politik-per-psychotrick-1.2386755.

Hoffmann, Christian/Schulz, Sönke E./Borchers, Kim Corinna, Grundrechtliche Wirkungsdimensionen im digitalen Raum. Bedrohungslagen im Internet und staatliche Reaktionsmöglichkeiten, MMR 2014, 89–95.

Hoffmann-Riem, Wolfgang, Öffentliches Recht und Privatrecht als wechselseitige Auffangordnungen. Systematisierung und Entwicklungsperspektiven, in: Hoffmann-Riem, Wolfgang/Schmidt-Aßmann, Eberhard (Hrsg.), Öffentliches Recht und Privatrecht als wechselseitige Auffangordnungen, Baden-Baden 1996, 261–336.

–, Grundrechts- und Funktionsschutz für elektronisch vernetzte Kommunikation, 134 AöR (2009), 513–541.

–, Informationelle Selbstbestimmung in der Informationsgesellschaft. Auf dem Wege zu einem neuen Konzept des Datenschutzes, in: ders. (Hrsg.), Offene Rechtswissenschaft – Ausgewählte Schriften von Wolfgang Hoffmann-Riem und begleitende Analysen, Tübingen 2010, 499–523.

–, Freiheitsschutz in den globalen Kommunikationsinfrastrukturen, JZ 2014, 53–63.

Höfling, Wolfram, Menschenwürde und gute Sitten, NJW 1983, 1582–1585.

Hohmann-Dennhardt, Christine, Freiräume – Zum Schutz der Privatheit, NJW 2006, 545–549.

Holznagel, Bernd, Regulierte Selbstregulierung im Medienrecht, in: Die Verwaltung Beiheft 4 – Regulierte Selbstregulierung als Steuerungskonzept des Gewährleistungsstaates, Berlin 2001, 81–100.

Horn, Hans-Detlef, Schutz der Privatsphäre, in: Isensee, Josef/Kirchhof, Paul (Hrsg.), Handbuch des Staatsrechts der Bundesrepublik Deutschland VII – Freiheitsrechte, 3. Aufl., Heidelberg 2009, 147–206.

Horn, Nikolai, Das Netz als ethische Herausforderung, 542 Politische Studien (2013), 54–60.

Hornung, Gerrit, Zwei runde Geburtstage: Das Recht auf informationelle Selbstbestimmung und das WWW, MMR 2004, 3–8.

–, Die kumulative Wirkung von Überwachungsmaßnahmen: Eine Herausforderung an die Evaluierung von Sicherheitsgesetzen, in: Albers, Marion/Weinzierl, Ruth (Hrsg.), Menschenrechtliche Standards in der Sicherheitspolitik – Beiträge zur rechtsstaatsorientierten Evaluierung von Sicherheitsgesetzen, Baden-Baden 2010, 65–85.

–, Datenschutz – nur solange der Vorrat reicht? Die Speicherung von Telekommunikationsverkehrsdaten als Problem der Abwägungskompetenz im Mehrebenensystem, PVS Sonderheft 46, 2012, 377–407.

–, Eine Datenschutzgrundverordnung für Europa? Licht und Schatten im Kommissionsentwurf vom 25.1.2012, ZD 2012, 99–106.

–, Die europäische Datenschutzreform, in: Scholz, Matthias/Funk, Axel (Hrsg.), DGRI Jahrbuch 2012, Köln 2013, 1–24.

–, Regulating privacy enhancing technologies: seizing the opportunity of the future European Data Protection Framework, 26 Innovation: The European Journal of Social Sciences (2013), 181–196.

–, Europa und darüber hinaus – Konzepte für eine Neuregelung des Datenschutzes im Internet und in sozialen Netzwerken, in: Hill, Hermann/Schliesky, Utz (Hrsg.), Die Neubestimmung der Privatheit – E-Volution des Rechts- und Verwaltungssystems IV, Baden-Baden 2014, 123–151.

–, Grundrechtsinnovationen, Tübingen 2015.

Hornung, Gerrit/Hartl, Korbinian, Datenschutz durch Marktanreize – auch in Europa? Stand der Diskussion zu Datenschutzzertifizierung und Datenschutzaudit, ZD 2014, 219–225.

Hornung, Gerrit/Hofmann, Kai, Ein „Recht auf Vergessenwerden"? Anspruch und Wirklichkeit eines neuen Datenschutzrechts, JZ 2013, 163–170.

Huster, Stefan, Individuelle Menschenwürde oder öffentliche Ordnung? Ein Diskussionsbeitrag anlässlich „Big Brother", NJW 2000, 3477–3479.

Internet & Gesellschaft Co:llaboratory, Gleichgewicht und Spannung zwischen digitaler Privatheit und Öffentlichkeit. Phänomene, Szenarien und Denkanstöße, Berlin 11.2011.

Isensee, Josef, Das Grundrecht auf Sicherheit. Zu den Schutzpflichten des freiheitlichen Verfassungsstaates, Berlin/New York 1983.

–, Privatautonomie, in: Isensee, Josef/Kirchhof, Paul (Hrsg.), Handbuch des Staatsrechts der Bundesrepublik Deutschland VII – Freiheitsrechte, 3. Aufl., Heidelberg 2009, 207–280.

–, Das Grundrecht als Abwehrrecht und als staatliche Schutzpflicht, in: Isensee, Josef/Kirchhof, Paul (Hrsg.), Handbuch des Staatsrechts der Bundesrepublik Deutschland X, 3. Aufl., Heidelberg 2012, 413–567.

Jandt, Silke/Roßnagel, Alexander, Social Networks für Kinder und Jugendliche. Besteht ein ausreichender Datenschutz?, MMR 2011, 637–642.

Jeand'Heur, Bernd, Grundrechte im Spannungsverhältnis zwischen subjektiven Freiheitsgarantien und objektiven Grundsatznormen. Zur Erweiterung der Grundrechtsfunktionen und deren Auswirkungen auf die Grundrechtsdogmatik, JZ 1995, 161–167.

Jellinek, Georg, System der subjektiven öffentlichen Rechte, Freiburg i. Br. 1892.

Jensen, Sarah, Irischer High Court legt EuGH Fragen zum Safe Harbor-Abkommen vor, ZD-Aktuell 2014, 04284.

Jernigan, Carter/Mistree, Behram F.T., Gaydar: Facebook friendships expose sexual orientation, 14 First Monday (2009).

Jerome, Joseph W., Buying and Selling Privacy: Big Data's Different Burdens and Benefits, 66 Stanford L. Rev. Online (2013), 47–53.

Johnson, Deborah G./Wayland, Kent A., Surveillance and transparency as sociotechnical systems of accountability, in: Haggerty, Kevin D./Samatas, Minas (Hrsg.), Surveillance and Democracy, New York 2010, 19–33.

Jolls, Christine, Rationality and Consent in Privacy Law, 2010, http://www.law.yale.edu/documents/pdf/Alumni_Affairs/Jolls_RationalityandConsentinPrivacyLaw_1-21-10.pdf.

Jolls, Christine/Sunstein, Cass R./Thaler, Richard H., A Behavioral Approach to Law and Economics, 50 Stanford L. Rev. Online (1998), 1471–1550.

Jones, Rhys/Pykett, Jessica/Whitehead, Mark, Governing temptation: Changing behaviour in an age of libertarian paternalism, 35 Progress in Human Geography (2011), 483–501.

Joost, Nine, Begrenzte Rationalität und ärztliche Aufklärungspflichten. Soll das Recht dem Risiko defizitärer Patiententenentscheidungen entgegenwirken?, in: Fateh-Moghadam, Bijan/Sellmaier, Stephan/Vossenkuhl, Wilhelm (Hrsg.), Grenzen des Paternalismus, Stuttgart 2010, 126–159.

Jürgens, Pascal/Stark, Birgit/Magin, Melanie, Gefangen in der Filter Bubble? Search Engine Bias und Personalisierungsprozesse bei Suchmaschinen, in: Stark, Birgit/Dörr, Dieter/Aufenanger, Stefan (Hrsg.), Die Googleisierung der Informationssuche – Suchmaschinen zwischen Nutzung und Regulierung, Berlin 2014, 98–135.

Juris Redaktion, EuGH-Gutachten: Entwurf der Übereinkunft über EU-Beitritt zur EMRK unionsrechtswidrig, 18.12.2014, https://www.juris.de/jportal/portal/page/homerl.psml?nid=jnachr-JUNA141203286&cmsuri=%2Fjuris%2Fde%2Fnachrichten%2Fzeigenachricht.jsp.

Justice Scalia, Antonin, Constitutional Interpretation the Old Fashioned Way. Justice Antonin Scalia delivered the following remarks at the Woodrow Wilson International Center for Scholars in Washington, D.C. 14.3.2005, http://www.cfif.org/htdocs/freedomline/current/guest_commentary/scalia-constitutional-speech.htm.

Kahmann, Katharina, Überwachen und Strafen im Internet, in: Venhaus, Marc/Haselbeck, Sebastian/Wintermann, Ole (Hrsg.), Globalisierung im Schatten der Überwachung – Internet. Demokratie. Handel, Berlin 2013, 65–67.

Kahneman, Daniel, Thinking, Fast and Slow, New York 2011.

Kamlah, Ruprecht B., Right of Privacy. Das allgemeine Persönlichkeitsrecht in amerikanischer Sicht unter Berücksichtigung neuer technologischer Entwicklungen, Köln/Berlin/Bonn/München 1969.

–, Hinweise aus der Rechtsprechung des Bundesverfassungsgerichts zur Regelung eines materiellen Informationsrechts, in: Steinmüller, Wilhelm (Hrsg.), Informationsrecht und Informationspolitik, München, Wien 1976, 196–206.

Kang, Jerry, Information Privacy in Cyberspace Transactions, 50 Stanford L. Rev. Online (1998), 1193–1194.

Kang, Jerry/Buchner, Benedikt, Privacy in Atlantis, 18 Harvard J. of L. and Tech. (2004), 230–267.

Kappes, Christopher, Warum die Gefahren der Filter Bubble überschätzt werden, 5.2012, http://christophkappes.de/wp-content/uploads/downloads/2012/06/TZD_Kappes-Christoph_-Filter-Bubble.pdf.

Kapsner, Andreas/Sandfuchs, Barbara, Nudging as a Threat to Privacy, 6 Rev. of Philosophy and Psychology (2015), 455–468.

Käß, Robert, Das Urteil des Bundesverfassungsgerichts zum Antiterrordateigesetz. Trennung von Grundrechtssphären und informationelles Trennungsprinzip, BayVBl 2013, 709–713.

Keighley, Jennifer M., Can You Handle The Truth? Compelled Commercial Speech and the First Amendment, 15 J. of Constitutional L. (2012), 539–617.

Kelbert, Florian/meh Shirazi, Fate/Simo, Hervais/Wüchner, Tobias/Buchmann, Johannes, State of Online Privacy: A Technical Perspective, in: Buchmann, Johannes (Hrsg.), Internet Privacy – Eine multidisziplinäre Bestandsaufnahme (acatech Studie), Berlin, Heidelberg 2012, 189–280.

Kerr, Ian/Earle, Jessica, Prediction, Preemption, Presumption: How Big Data Threatens Big Picture Privacy, 66 Stanford L. Rev. Online (2013), 65–72.

Kirste, Stephan, Harter und weicher Rechtspaternalismus. Unter besonderer Berücksichtigung der Medizinethik, JZ 2011, 805–814.

Klass, Nadine, Der Schutz der Privatsphäre durch den EGMR im Rahmen von Medienberichterstattungen. Zugleich Besprechung der dritten »Caroline von Hannover/Deutschland«-Entscheidung sowie der »Ruusunen/Finnland«-Entscheidung des EGMR, ZUM 2014, 261–269.

Klein, Andreas./Leithold, F./Zell, C./Roosen, J., Digitale Profilbildung und Gefahren für die Verbraucher. Zusammenfassung, München 2010.

Klein, Eckart, Grundrechtliche Schutzpflicht des Staates, NJW 1989, 1633–1640.

Klein, Hans H., Die Grundrechtliche Schutzpflicht, DVBl. 1994, 489–497.

Klein, Oliver, Das Untermaßverbot. Über die Justiziabilität grundrechtlicher Schutzpflichterfüllung, JuS 2006, 960–964.

Klick, Jonathan/Mitchell, Gregory, Government Regulation of Irrationality: Moral and Cognitive Hazards, 90 Minnesota L. Rev. (2006), 1620–1663.

Klinkhammer, Patrick/Müllejans, Gabi, Veröffentlichen von Fotos in sozialen Netzwerken – ein Überblick über mögliche Rechtsfolgen, ArbRAktuell 2014, 503–506.
Knyrim, Rainer, Entwurf der neuen EU-Datenschutz-Grundverordnung, in: Scholz, Matthias/Funk, Axel (Hrsg.), DGRI Jahrbuch 2012, Köln 2013, 25–38.
Köpernik, Kristin, Zur Notwendigkeit einer Verbandsklage bei Datenschutzverstößen, VuR 2014, 240–242.
Krempl, Stefan, Friedrich erhebt Sicherheit zum „Supergrundrecht“, 17.7.2013, http://www.heise.de/newsticker/meldung/Friedrich-erhebt-Sicherheit-zum-Supergrundrecht-1919309.html.
Krieger, Heike, Positive Verpflichtungen unter der EMRK: Unentbehrliches Element einer gemein-europäischen Grundrechtsdogmatik, leeres Versprechen oder Grenze der Justiziabilität?, ZaöRV 2014, 187–213.
Krings, Günter, Grund und Grenzen grundrechtlicher Schutzansprüche. Die subjektiv-rechtliche Rekonstruktion der grundrechtlichen Schutzpflichten und ihre Auswirkung auf die verfassungsrechtliche Fundierung des Verbrauchervertragsrechts, Berlin 2003.
Kühling, Jürgen/Gauß, Nicolaus, Suchmaschinen – eine Gefahr für den Informationszugang und die Informationsvielfalt?, ZUM 2007, 881–889.
Kuhn, Johannes, „Lobbyplag.eu“ zum Datenschutz. Mit der Handschrift von Lobbyisten. „Forum Shopping“ für die IT-Industrie?, 11.2.2013, http://www.sueddeutsche.de/politik/lobbyplageu-zum-datenschutz-mit-der-handschrift-von-lobbyisten-1.1596685.
Kumm, Matthias/Ferreres Comella, Víctor, What Is So Special about Constitutional Rights in Private Litigation? A Comparative Analysis of the Function of State Action Requirements and Indirect Horizontal Effect, in: Sajó, András/Uitz, Renáta (Hrsg.), The Constitution in Private Relations – Expanding Constitutionalism, Den Haag 2005, 241–299.
Künast, Renate, „Meine Daten gehören mir” – und der Datenschutz gehört ins Grundgesetz, ZRP 2008, 201–205.
Kutscha, Martin, Mehr Datenschutz – aber wie?, ZRP 2010, 112–114.
–, Grundrechtlicher Persönlichkeitsschutz bei der Nutzung des Internets. Zwischen individueller Selbstbestimmung und staatlicher Verantwortung, DuD 2011, 461–464.
–, Erster Teil, in: Kutscha, Martin/Thomé, Sarah (Hrsg.), Grundrechtsschutz im Internet?, Baden-Baden 2013, 11–100.
Ladeur, Karl-Heinz, Die Regulierung von Selbstregulierung und die Herausbildung einer „Logik der Netzwerke“. Rechtliche Steuerung und die beschleunigte Selbsttransformation der postmodernen Gesellschaft, in: Die Verwaltung Beiheft 4 – Regulierte Selbstregulierung als Steuerungskonzept des Gewährleistungsstaates, Berlin 2001, 59–77.
Lange, Friederike Valerie, Grundrechtsbindung des Gesetzgebers. Eine rechtsvergleichende Studie zu Deutschland, Frankreich und den USA, Tübingen 2010.
Langner, Thomas, Die Problematik der Geltung der Grundrechte zwischen Privaten, Frankfurt am Main 1998.
Leisner, Walter, Grundrechte und Privatrecht, München 1960.
Lemley, Mark A./McGowan, David, Legal Implications of Network Economic Effects, 86 California L. Rev. (1998), 479–611.
Lerman, Jonas, Big Data and its Exclusions, 66 Stanford L. Rev. Online (2013), 55–63.
Lessig, Lawrence, Code. version 2.0, New York 2006.
Levin, Irwin P./Gaeth, Gary J., How Consumers Are Affected by the Framing of Attribute Information Before and After Consuming a Product, 15 J. of Consumer Research (1988), 374–378.

Lewandowski, Dirk/Kerkmann, Friederike/Sünkler, Sebastian, Wie Nutzer im Suchprozess gelenkt werden. Zwischen technischer Unterstützung und interessengeleiteter Darstellung, in: Stark, Birgit/Dörr, Dieter/Aufenanger, Stefan (Hrsg.), Die Googleisierung der Informationssuche – Suchmaschinen zwischen Nutzung und Regulierung, Berlin 2014, 75–97.

Lin, Elbert, Prioritizing Privacy: A Constitutional Response to the Internet, 17 Berkeley Tech. L. J. (2002), 1085–1153.

Lisken, Hans, Freispruch für „Gurtmuffel" – ein Polizeiproblem?, NJW 1985, 3053–3056.

Littwin, Frank, Grundrechtsschutz gegen sich selbst. Das Spannungsverhältnis von grundrechtlichem Selbstbestimmungsrecht und Gemeinschaftsbezogenheit des Individuums, Frankfurt am Main 1993.

Lobosco, Katie, Facebook friends could change your credit score, 27.8.2013, http://money.cnn.com/2013/08/26/technology/social/facebook-credit-score/index.html?hpt=hp_t2.

Loewenstein, Karl, Verfassungsrecht und Verfassungspraxis der Vereinigten Staaten, Berlin/Göttingen/Heidelberg 1959.

Lucas, Gary, JR., Saving Smokers From Themselves: The Paternalistic Use of Cigarette Taxes, 80 Univ. of Cincinnati L. Rev. (2012), 693–751.

Lüdemann, Jörn, Die Grenzen des homo oeconomicus und die Rechtswissenschaft, in: Engel, Christoph/Englerth, Markus/Lüdemann, Jörn/Spiecker genannt Döhmann, Indra (Hrsg.), Recht und Verhalten – Beiträge zu Behavioral Law and Economics, Tübingen 2007, 7–59.

Luhmann, Niklas, Grundrechte als Institution. Ein Beitrag zur politischen Soziologie, Berlin 1965.

Lutterbeck, Bernd, Komplexe Kontexte – einfache Regeln. Zwischen Liberalität und Paternalismus – Wo fördert, wo beschränkt der Datenschutz Bürgerrechte?, in: Mehde, Veith/Ramsauer, Ulrich/Seckelmann, Margit (Hrsg.), Staat, Verwaltung, Information – Festschrift für Hans Peter Bull zum 75. Geburtstag, Berlin 2011, 1017–1028.

Maisch, Michael Marc, Informationelle Selbstbestimmung in Netzwerken. Rechtsrahmen, Gefährdungslagen und Schutzkonzepte am Beispiel von Cloud Computing und Facebook, Berlin 2015.

Mangoldt, Herrmann v./Klein, Friedrich (Hrsg.), Kommentar zum Grundgesetz Band I. Präambel, Artikel 1 bis 19, 6. Aufl., München 2010.

Marthews, Alex/Tucker, Catherine, Government Surveillance and Internet Search Behavior, 24.03.2014, http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2412564.

Masing, Johannes, Herausforderungen des Datenschutzes, NJW 2012, 2305–2311.

Mattioli, Dana, On Orbitz, Mac Users Steered to Pricier Hotels, 6.6.2012, http://online.wsj.com/news/articles/SB10001424052702304458604577488822667325882#.

Maunz, Theodor/Dürig, Günter (Hrsg.), Grundgesetz. Kommentar Band I, 73. Aufl., München 12.2014 (zit. Maunz/Dürig-GG/*Bearbeiter*).

Mayer, Matthias, Untermaß, Übermaß und Wesensgehaltgarantie. Die Bedeutung staatlicher Schutzpflichten für den Gestaltungsspielraum des Gesetzgebers im Grundrechtsbereich, Baden-Baden 2005.

Mayer-Ladewig, Jens (Hrsg.), Europäische Menschenrechtskonvention. Handkommentar, 3. Aufl., Baden-Baden 2011.

Mayer-Schönberger, Viktor/Cukier, Kenneth, Big Data. A Revolution That Will Transform How We Live, Work and Think, London 2013.

Mayr, Erasmus, Grenzen des weichen Paternalismus II. Zwischen Harm-Principle und Unvertretbarkeit, in: Fateh-Moghadam, Bijan/Sellmaier, Stephan/Vossenkuhl, Wilhelm (Hrsg.), Grenzen des Paternalismus, Stuttgart 2010, 48–72.

McDonald, Aleecia/Faith Cranor, Lorrie, The Cost of Reading Privacy Policies, 4 I/S: A Journal of Law and Policy for the Information Society (2008), 540–565.

Merten, Detlef, Verhältnismäßigkeitsgrundsatz, in: Merten, Detlef/Papier, Hans-Jürgen (Hrsg.), Handbuch der Grundrechte in Deutschland und Europa III, Heidelberg 2009, 517–567.

Meyer, Jürgen (Hrsg.), Charta der Grundrechte der Europäischen Union, 4. Aufl., Baden-Baden 2014 (zit. Meyer-GRCh/*Bearbeiter*).

– (Hrsg.), EMRK. Europäische Menschenrechtskonvention Handkommentar, 3. Aufl., Baden-Baden 2011.

Mill, John Stuart, Über die Freiheit. Aus dem Englischen übersetzt von Bruno Lemke, Stuttgart 2010 (Original: 1859).

Mitchell, Gregory, Libertarian Paternalism Is an Oxymoron, 5.2002 FSU College of Law, Law and Economics Paper, 1–42.

Mitrou, Lilian, The impact of communications data retention on fundamental rights and democracy – the case of the EU Data Retention Directive, in: Haggerty, Kevin D./Samatas, Minas (Hrsg.), Surveillance and Democracy, New York 2010, 127–147.

Moore, Adam D., Privacy: Its Meaning and Value, 40 American Philosophical Quarterly (2003), 215–227.

–, Coercing Privacy and Moderate Paternalism: Allen on Unpopular Privacy, 13 Philosophy and Law (2013), 10–14.

Mowbray, Alastair, The Development of Positive Obligations under the European Convention on Human Rights by the European Court of Human Rights, Oxford/Portland 2004.

Müller, Günter/Flender, Christian/Peters, Martin, Vertrauensinfrastruktur und Privatheit als ökonomische Fragestellung, in: Buchmann, Johannes (Hrsg.), Internet Privacy – Eine multidisziplinäre Bestandsaufnahme (acatech Studie), Berlin, Heidelberg 2012, 143–189.

Mullin, Joe, Microsoft agrees to contempt order so e-mail privacy case can be appealed, 10.9.2014, http://arstechnica.com/tech-policy/2014/09/microsoft-agrees-to-contempt-order-so-e-mail-privacy-case-can-be-appealed/.

Münch, Ingo von, Grundrechtsschutz gegen sich selbst?, in: Stödter, Rolf/Thieme, Werner (Hrsg.), Festschrift für Hans Peter Ipsen zum siebzigsten Geburtstag – Hamburg. Deutschland. Europa, Tübingen 1977, 113–128.

Murswiek, Dietrich, Das Bundesverfassungsgericht und die Dogmatik mittelbarer Grundrechtseingriffe. Zu der Glykol- und der Osho- Entscheidung vom 26.6.2002, NVwZ 2003, 1–8.

Nagenborg, Michael, Diskretion in offenen Netzen. IuK-Handlungen und die Grenze zwischen dem Privaten und dem Öffentlichen, in: Spinner, Helmut F./Nagenborg, Michael/Weber, Karsten (Hrsg.), Bausteine zu einer neuen Informationsethik, Berlin, Wien 2001, 93–128.

–, Das Private unter den Rahmenbedingungen der IuK-Technologie. Ein Beitrag zur Informationsethik, Wiesbaden 2005.

Nehf, James P., Recognizing the Societal Value in Information Privacy, 78 Washington L. Rev. (2003), 1–92.

–, Shopping for Privacy Online: Consumer Decision Making Strategies and the Emerging Market for Information Privacy, 1 Univ. of Illinios J. of L., Tech. and Policy (2005), 1–50.

Nettesheim, Martin, Grundrechtsschutz der Privatheit, in: Höfling, Wolfram (Hrsg.), Der Schutzauftrag des Rechts – Referate und Diskussionen auf der Tagung der Vereinigung der Deutschen Staatsrechtslehrer in Berlin vom 29. September bis 2. Oktober 2010, Berlin 2011, 7–49.

Newman, Nathan, Search, Antitrust and the Economics of the Control of User Data, 30 Yale J. on Regulation (2014), 401–474.

–, The Costs of Lost Privacy: Consumer Harm and Rising Economic Inequality in the Age of Google, 40 William Mitchell L. Rev. (2014), 849–889.

Nietsch, Thomas, Zur Überprüfung des Datenschutzrechts durch Verbraucherverbände, CR 2014, 272–278.

Nink, Judith/Laue, Philip, Anmerkung zu LG Frankfurt/M., CR 2014, 269–271.

Nipperdey, Hans Carl, Grundrechte und Privatrecht, Krefeld 1961.

Nissenbaum, Helen, Privacy as Contextual Integrity, 79 Washington L. Rev. (2004), 119–156.

–, Privacy in context. Technology, policy, and the integrity of social life, Stanford 2010.

–, A Contextual Approach to Privacy Online, Daedalus, the Journal of the American Academy of Arts & Sciences 2011, 32–48.

Nußberger, Angelika, Das Verhältnismäßigkeitsprinzip als Strukturprinzip richterlichen Entscheidens in Europa, NVwZ-Beilage 2013, 36–44.

Oermann, Markus/Staben, Julian, Mittelbare Grundrechtseingriffe durch Abschreckung. Zur grundrechtlichen Bewertung polizeilicher „Online-Streifen" und „Online-Ermittlungen" in sozialen Netzwerken, 52 Der Staat (2013), 630–661.

Ohrtmann, Jan-Peter/Schwiering, Sebastian, Big Data und Datenschutz – Rechtliche Herausforderungen und Lösungsansätze, NJW 2014, 2984–2989.

Olshausen, Henning von, Menschenwürde im Grundgesetz: Wertabsolutismus oder Selbstbestimmung?, NJW 1982, 2221–2224.

Opsahl, Kurt, Why Metadata matters, 7.6.2013, https://www.eff.org/deeplinks/2013/06/why-metadata-matters.

Orwell, George, Nineteen Eighty-Four, Essex 1990 (Original: 1949).

Oskamp, Stuart, Overconfidence in case-study judgments, in: Kahneman, Daniel/Slovic, Paul/Tversky, Amos (Hrsg.), Judgement under uncertainty: Heuristics and biases, Cambridge 1982, 287–293.

Oswald, Katja, Weicher Paternalismus und das Verbot der Teilnahme untergebrachter Personen an klinischen Arzneimittelprüfungen, in: Fateh-Moghadam, Bijan/Sellmaier, Stephan/Vossenkuhl, Wilhelm (Hrsg.), Grenzen des Paternalismus, Stuttgart 2010, 94–125.

Ott, Stephan, Schutz der Nutzerdaten bei Suchmaschinen Oder: Ich weiß, wonach du letzten Sommer gesucht hast …, MMR 2009, 448–453.

Paal, Boris, Vielfaltsicherung im Suchmaschinensektor, ZRP 2015, 34–38.

Papier, Hans-Jürgen, Drittwirkung der Grundrechte, in: Merten, Detlef/Papier, Hans-Jürgen (Hrsg.), Handbuch der Grundrechte in Deutschland und Europa II – Grundrechte in Deutschland: Allgemeine Lehren I, Heidelberg 2006, 1331–1360.

Pariser, Eli, The Filter Bubble, 10.10.2010, http://www.theatlantic.com/daily-dish/archive/2010/10/the-filter-bubble/181427/.

–, Filter Bubble. Wie wir im Internet entmündigt werden, München 2012.

Parker, Clifton B., Stanford students show that phone record surveillance can yield vast amounts of information, 12.3.2014, https://news.stanford.edu/news/2014/march/nsa-phone-surveillance-031214.html.

Parker, Richard B., A Definition of Privacy, 27 Rutgers L. Rev. (1974), 275–296.

Pietzcker, Jost, Die Rechtsfigur des Grundrechtsverzichts, 17 Der Staat (1978), 527–551.

Podlech, Adalbert, Verfassungsrechtliche Probleme öffentlicher Informationssysteme, 1 DVR (1972/73), 149–169.

–, Aufgaben und Problematiken des Datenschutzes, 5 DVR (1976), 23–39.

–, Das Recht auf Privatheit, in: Perels, Joachim (Hrsg.), Grundrechte als Fundament der Demokratie, Frankfurt am Main 1979, 50–67.
Polonetsky, Jules/Tene, Omer, Privacy and Big Data: Making Ends Meet, 66 Stanford L. Rev. Online (2013), 25–33.
Pomeranz, Jennifer L., Compelled Speech Under the Commercial Speech Doctrine: The Case of Menu Label Laws, 12 J. of Health Care L. & Policy (2009), 159–194.
Porat, Ariel/Strahilevitz, Lior Jacob, Personalizing Default Rules and Disclosure with Big Data, 112 Mich. L. Rev. (2014), 1417–1478.
Porksen, Bernhard/Detel, Hanne, Der entfesselte Skandal. Das Ende der Kontrolle im digitalen Zeitalter, Köln 2012.
Posner, Richard A., The Right of Privacy, 12 Georgia L. Rev. (1978), 393–422.
–, Economic Analysis of Law, 7. Aufl., New York 2007.
Post, Claudia, Yellow Press and Privacy: Die Rechtsprechung des US Supreme Court, GRUR Int 2006, 283–292.
Post, Robert C., The Social Foundations of Privacy: Community and Self in the Common Law Tort, 77 California L. Rev. (1989), 957–1010.
Prosser, William L., Privacy, 48 California L. Rev. (1960), 383–423.
Rabel, Ernst, Aufgabe und Notwendigkeit der Rechtsvergleichung, München 1925.
Radin, Margaret Jane, Market-Inalienability, 100 Harvard L. Rev. (1987), 1849–1937.
Radlanski, Philip, Das Konzept der Einwilligung in der datenschutzrechtlichen Realität, Tübingen 2015 (im Erscheinen).
Rainie, Lee/Madden, Mary, Americans' Privacy Strategies Post-Snowden, 16.3.2015, http://www.pewinternet.org/2015/03/16/Americans-Privacy-Strategies-Post-Snowden/.
Redaktion beck-aktuell, Gesetzentwurf: Kabinett beschließt Verbandsklagerecht bei missbräuchlicher Verwendung von Verbraucherdaten, becklink 4.2.2015, 1036989.
–, De Maizière für «digitalen Radiergummi» im Internet, becklink 23.6.2010, 1002049.
–, Aigner schlägt Verfallsdatum für Internet-Dateien vor, becklink 10.1.2011, 1008988.
Redaktion FD-ArbR, Jedes zweite Unternehmen überprüft Bewerber in Sozialen Netzwerken, FD-ArbR 2015, 369739.
Redaktion MMR-Aktuell, Vorratsdatenspeicherung im Gesetzgebungsverfahren, MMR-Aktuell 2015, 369589.
Redaktion ZD-Aktuell, EuGH: Terminhinweis, ZD-Aktuell 2015, 04593.
Redeker, Helmut, IT-Recht, 5. Aufl., München 2012.
Regan, Priscilla M., Legislating Privacy: Technology, Social Values, and Public Policy, Chapel Hill/London 1995.
Reuters Institute for the Study of Journalism, Reuters Institute Digital News Report 2014, Oxford 2014.
Rheinstein, Max, Einführung in die Rechtsvergleichung. bearbeitet, herausgegeben und eingeleitet von Reimer von Borries, München 1974.
Richards, Neil M., Intellectual Privacy, 87 Texas L. Rev. (2008), 387–445.
–, The Dangers of Surveillance, 126 Harvard L. Rev. (2013), 1934–1965.
Richards, Neil M./King, Jonathan H., Three Paradoxes of Big Data, 66 Stanford L. Rev. Online (2013), 41–46.
Rizzo, Mario J./Whitman, Douglas Glen, Little Brother is Watching You: New Paternalism on the Slippery Slopes, 51 Arizona L. Rev. (2009), 685–739.
Rogosch, Patricia Maria, Die Einwilligung im Datenschutzrecht, Baden-Baden 2013.
Rose-Ackerman, Susan, Inalienability and The Theory of Property Rights, 85 Columbia L. Rev. (1985), 931–969.

Rosen, Jeffrey, The Right to be Forgotten, 64 Stanford L. Rev. Online (2012), 88.
–, Madison's Privacy Blind Spot, 18.1.2014, http://www.nytimes.com/2014/01/19/opinion/sunday/madisons-privacy-blind-spot.html?_r=0.
Rössler, Beate, Der Wert des Privaten, Frankfurt am Main 2001.
–, Der Wert des Privaten: Lieberale Theorie und Gesellschaftskritik, in: Jurczyk, Karin (Hrsg.), Das Private neu denken – Erosionen, Ambivalenzen, Leistungen, Münster 2008, 282–300.
–, Privatheit, in: Gosepath, Stefan/Hinsch, Wilfried/Rössler, Beate (Hrsg.), Handbuch der Politischen Philosophie und Sozialphilosophie, Berlin 2008, 1023–1030.
–, Autonomy, Paternalism, and Privacy. Some Remarks on Anita Allen, 13 Philosophy and Law (2013), 14–19.
Rössler, Beate/Mokrosinska, Dorota, Privacy and social interaction, 39 Philosophy and Social Criticism (2013), 772–791.
Roßnagel, Alexander, Datenschutzaudit. Konzeption, Durchführung, gesetzliche Regelung, Braunschweig/Wiesbaden 2000.
–, Konzepte des Selbstdatenschutzes, in: ders. (Hrsg.), Handbuch Datenschutzrecht – Die neuen Grundlagen für Wirtschaft und Verwaltung, München 2003, 325–362.
–, Datenschutz in einem informatisierten Alltag, Berlin 2007.
–, Big Data – Small Privacy? Konzeptionelle Herausforderungen für das Datenschutzrecht, ZD 2013, 562–566.
Roßnagel, Alexander/Pfitzmann, Andreas/Garstka, Hansjürgen, Modernisierung des Datenschutzrechts. Gutachten im Auftrag des Bundesministeriums des Innern, Berlin 2001.
–/–/–, Modernisierung des Datenschutzrechts, DuD 2001, 253–263.
Roßnagel, Alexander/Scholz, Philip, Datenschutz durch Anonymität und Pseudonymität. Rechtsfolgen der Verwendung anonymer und pseudonymer Daten, MMR 2000, 721.
Rostron, Allen, Pragmatism, Paternalism, and the Constitutional Protection of Commercial Speech, 37 Vermont L. Rev. (2013), 529–589.
Rotenberg, Marc, Fair Information Practices and the Architecture of Privacy. (What Larry Doesn't Get), 1 Stanford Tech. L. Rev. (2001), 1–34.
Rotenberg, Marc/Jacobs, David, Updating the Law of Information Privacy: The New Framework of the European Union, 36 Harvard J. of L. and Public Policy (2013), 606–652.
Roth, Wolfgang, Faktische Eingriffe in Freiheit und Eigentum. Struktur und Dogmatik des Grundrechtstatbestandes und der Eingriffsrechtfertigung, Berlin 1994.
Rubinstein, Ira S./Lee, Ronald D./Schwartz, Paul M., Data Mining and Internet Profiling: Emerging Regulatory and Technological Approaches, 75 Chicago L. Rev. (2008), 261–285.
Rudolf, Walter, Recht auf informationelle Selbstbestimmung, in: Merten, Detlef/Papier, Hans-Jürgen (Hrsg.), Handbuch der Grundrechte in Deutschland und Europa IV – Grundrechte in Deutschland: Einzelgrundrechte I, Heidelberg 2011, 233–289.
Rüpke, Giselher, Der verfassungsrechtliche Schutz der Privatheit. Zugleich ein Versuch pragmatischen Grundrechtsverständnisses, Baden-Baden 1976.
Rupp, Martin, Die grundrechtliche Schutzpflicht des Staates für das Recht auf informationelle Selbstbestimmung im Pressesektor, Saarbrücken 2013.
Sacco, Rodolfo, Einführung in die Rechtsvergleichung. Aus dem Italienischen übersetzt von Dr. Jacob Joussen, Baden-Baden 2001.
Sachs, Michael, The Duty to Protect and to Ensure Human Rights Under the Basic Law of the Federal Republic of Germany, in: Klein, Eckart (Hrsg.), The Duty to Protect and to Ensure Human Rights – Colloquium Potsdam, 1–3 July 1999, Berlin 2000, 53–72.

Saletan, William, Bubble Think. How to escape a partisan echo chamber, 3.5.2010, http://www.slate.com/articles/news_and_politics/frame_game/2010/05/bubble_think.html.
Sandfuchs, Barbara, Exclusionary Conduct and the Proposed Right to Data Portability, 16.5.2014, http://comparativecompetition.blog.com/2014/05/16/exclusionary-conduct/.
–, Privacy Nudges, in: Akrivopoulou, Christina (Hrsg.), Protecting the Genetic Self from Biometric Threats – Autonomy, Identity, and Genetic Privacy, Hershey 2015, 256–264.
–, Rezension, Schliesky/Schulz, Schutzpflichten und Drittwirkung im Internet, MMR-Aktuell 2015, 365281.
Sandfuchs, Barbara/Kapsner, Andreas, Coercing Online Privacy, 11 I/S: A Journal of Law and Policy for the Information Society (2016) (im Erscheinen).
Schaar, Peter, Lässt sich die globale Internetüberwachung noch bändigen?, ZRP 2013, 214–216.
Schaller, Werner, Das Verhältnis von EMRK und deutscher Rechtsordnung vor und nach dem Beitritt der EU zur EMRK, EuR 2006, 656–674.
Schatzschneider, Wolfgang, Rechtsordnung und Prostitution. Einige Anmerkungen zur staatlichen Reglementierung des „ältesten Gewerbes", NJW 1985, 2793–2797.
Schaub, Günter (Hrsg.), Arbeitsrechtshandbuch. Systematische Darstellung und Nachschlagewerk für die Praxis, 15. Aufl., München 2013.
Schiedermair, Stephanie, Der Schutz des Privaten als internationales Grundrecht, Tübingen 2012.
Schliesky, Utz/Hoffmann, Christian/Luch, Anika D./Schulz, Sönke E./Borchers, Kim Corinna, Schutzpflichten und Drittwirkung im Internet. Das Grundgesetz im digitalen Zeitalter, Baden-Baden 2014.
Schmidt, Manfred G., Demokratietheorien. Eine Einführung, 4. Aufl., Wiesbaden 2008.
Schmidt-Aßmann, Eberhard, Regulierte Selbstregulierung als Element verwaltungsrechtlicher Systembildung, in: Die Verwaltung Beiheft 4 – Regulierte Selbstregulierung als Steuerungskonzept des Gewährleistungsstaates, Berlin 2001, 253–271.
Schmies, Christian, Behavioral Finance und Finanzmarktregulierung, in: Engel, Christoph/Englerth, Markus/Lüdemann, Jörn/Spiecker genannt Döhmann, Indra (Hrsg.), Recht und Verhalten – Beiträge zu Behavioral Law and Economics, Tübingen 2007.
Schmitt, Stefan, Automatisch vorsortiert, 22.6.2011, http://www.zeit.de/2011/26/Internet-Surfverhalten-Filter.
Schnabel, Christoph, Datenschutz bei profilbasierten Location Based Services. Die datenschutzadäquate Gestaltung von Service-Plattformen für Mobilkommunikation, Kassel 2009.
Schneider, Adrian, EU-Kommission: Cookie-Richtlinie ist in Deutschland umgesetzt, 5.2.2014, http://www.telemedicus.info/article/2716-EU-Kommission-Cookie-Richtlinie-ist-in-Deutschland-umgesetzt.html.
Schneider, Hans Peter, Eigenart und Funktionen der Grundrechte im demokratischen Verfassungsstaat, in: Perels, Joachim (Hrsg.), Grundrechte als Fundament der Demokratie, Frankfurt am Main 1979, 11–49.
Schneider, Jochen/Härting, Niko, Datenschutz in Europa – Plädoyer für einen Neubeginn. Zehn „Navigationsempfehlungen", damit das EU-Datenschutzrecht internettauglich und effektiv wird, CR 2014, 306–312.
Schoch, Friedrich, Die Schwierigkeiten des BVerfG mit der Bewältigung staatlichen Informationshandelns, NVwZ 2011, 193–198.

Scholz, Philip, Datenschutz bei Data Warehousing und Data Mining, in: Roßnagel, Alexander (Hrsg.), Handbuch Datenschutzrecht – Die neuen Grundlagen für Wirtschaft und Verwaltung, München 2003, 1833–1875.

Schröder, Christian, Die Haftung für Verstöße gegen Privacy Policies und Codes of Conduct nach US-amerikanischem und deutschem Recht. Zugleich ein Beitrag zur Rechtsnatur von Datenschutzerklärungen, Verhaltensregeln gem. § 38a BDSG und Unternehmensregelungen gem. § 4c Abs. 2 BDSG, Baden-Baden 2007.

Schroth, Ulrich, Die Begrenzung des Spenderkreises im Transplantationsgesetz als Problem der paternalistischen Einschränkung menschlicher Freiheit, in: Schünemann, Bernd/Müller, Jörg Paul/Philipps, Lothar (Hrsg.), Das Menschenbild im weltweiten Wandel der Grundrechte, Berlin 2002, 35–44.

Schulhofer, Stephen J., More Essential Than Ever: The Fourth Amendment in the Twenty First Century, New York 2012.

Schulz, Wolfgang, Regulierte Selbstregulierung im Telekommunikationsrecht. Die informationale Beteiligung Dritter bei der Besetzung des Regulierers in Deutschland und den Vereinigten Staaten, in: Die Verwaltung Beiheft 4 – Regulierte Selbstregulierung als Steuerungskonzept des Gewährleistungsstaates, Berlin 2001, 101–122.

Schwabe, Jürgen, Die sogenannte Drittwirkung der Grundrechte. Zur Einwirkung der Grundrechte auf den Privatrechtsverkehr, München 1971.

–, Der Schutz des Menschen vor sich selbst, JZ 1998, 66–75.

Schwabenbauer, Thomas, Heimliche Grundrechtseingriffe. Ein Beitrag zu Möglichkeiten und Grenzen sicherheitsbehördlicher Ausforschung, Tübingen 2013.

Schwartz, Paul M., The Computer in German and American Constitutional Law. Towards an American Right of Informational Self-Determination, 37 American J. of Comparative L. (1989), 675–701.

–, Das Übersetzen im Datenschutzrecht: Unterschiede zwischen deutschen und amerikanischen Konzepten der „Privatheit“, in: Frank, Armin P./Maaß, Kurt-Jürgen/Paul, Fritz (Hrsg.), Übersetzen, verstehen, Brücken bauen – Geisteswissenschaftliches und literarisches Übersetzen im internationalen Kulturaustausch, Band 1, Berlin 1993, 366–375.

–, Privacy and Democracy in Cyberspace, 52 Vanderbilt L. Rev. (1999), 1607–1702.

–, Beyond Lessig's Code for Internet Privacy: Cyberspace Filters, Privacy-Control, and Fair Information Practices Wisconsin L. Rev. 2000, 743–788.

–, Internet Privacy and the State, 32 Connecticut L. Rev. (2000), 815–859.

–, Property, Privacy, and Personal Data, 117 Harvard L. Rev. (2004), 2055.

–, Privacy Inalienability and the Regulation of Spyware, 20 Berkeley Tech. L.J. (2005), 1269–1282.

–, The EU-U.S. Privacy Collision: A Turn to Institutions and Procedures, 126 Harvard L. Rev. (2013), 1–43.

Schwartz, Paul M./Solove, Daniel J., Reconciling Personal Information in the United States and European Union, 3.5.2013 UC Berkeley Public Law Research Paper, 2271442.

–/–, The PII Problem: Privacy and a New Concept of Personally Identifiable Information, 86 New York Univ. L. Rev. (2011), 1814–1894.

Seubert, Sandra, Der gesellschaftliche Wert des Privaten, DuD 2012, 100–104.

Sidhu, Dawinder S., The Chilling Effect of Government Surveillance Programs on the Use of the Internet by Muslim-Americans, 7 Univ. of Maryland L.J. of Race, Religion, Gender (2007), 375–393.

Simitis, Spiros, Die informationelle Selbstbestimmung – Grundbedingung einer verfassungskonformen Informationsordnung, NJW 1984, 394–405.

–, Selbstbestimmung – Illusorisches Projekt oder reale Chance?, KJ 1988, 32–50.
– (Hrsg.), Bundesdatenschutzgesetz, 8. Aufl., Baden-Baden 2014.
Slobogin, Christopher, Public Privacy: Camera Surveillance of Public Places and the Right to Anonymity, 72 Mississippi. L. J. (2002), 213–299.
Slobogin, Christopher/Schumacher, Joseph E., Reasonable Expectations of Privacy and Autonomy in Fourth Amendment Cases: An Empirical Look at "Understandings Recognized and Permittet by Society", 42 Duke L. J. (1993), 727.
Smith, Aaron, 6 New Facts About Facebook, 3.2.2014, http://www.pewresearch.org/fact-tank/2014/02/03/6-new-facts-about-facebook/.
Sofsky, Wolfgang, Verteidigung des Privaten. Eine Streitschrift, München 2009.
Solove, Daniel J., Privacy and Power: Computer Databases and Metaphors for Information Privacy, 53 Stanford L. Rev. Online (2001), 1393–1462.
–, Conceptualizing Privacy, 90 California L. Rev. (2002), 1087–1155.
–, A Taxonomy of Privacy, 154 Univ. of Pennsylvania L. Rev. (2006), 477–560.
–, "I've Got Nothing to Hide" and Other Misunderstandings of Privacy, 44 San Diego L. Rev. (2007), 745–772.
–, Understanding Privacy, Cambridge/London 2009.
–, Nothing to Hide. The False Tradeoff between Privacy and Security, New Haven/London 2011.
–, Privacy Self-Management and the Consent Dilemma, 126 Harvard L. Rev. (2013), 1880–1903.
Solove, Daniel J./Schwartz, Paul M., Information Privacy Law, 3. Aufl., New York 2009.
–/–, Privacy Law Fundamentals, Portsmouth 2013.
Specht, Louisa, Konsequenzen der Ökonomisierung informationeller Selbstbestimmung – Die zivilrechtliche Erfassung des Datenhandels, in: Scholz, Matthias/Funk, Axel (Hrsg.), DGRI Jahrbuch 2012, Köln 2013, 239–247.
Spies, Axel, Berufungsverfahren Microsoft v. USA – Zugriff auf in Irland gelagerte Daten, ZD-Aktuell 2015, 04558.
Spindler, Gerald, IT-Sicherheit. Rechtliche Defizite und rechtspolitische Alternativen, MMR 2008, 7–13.
–, Persönlichkeitsschutz im Internet – Anforderungen und Grenzen einer Regulierung, in: Ständige Deputation des Deutschen Juristentages (Hrsg.), Verhandlungen des 69. Deutschen Juristentages, I, München 2012, F1-F136.
Spindler, Gerald/Schuster, Fabian (Hrsg.), Recht der elektronischen Medien, 3. Aufl., München 2015.
Starck, Christian, Grundrechtliche und demokratische Freiheitsidee, in: Isensee, Josef/Kirchhof, Paul (Hrsg.), Handbuch des Staatsrechts der Bundesrepublik Deutschland III – Demokratie – Bundesorgane, 3. Aufl., Heidelberg 2005, 3–29.
Steiger, J., Entwicklungen im Grundrechtsverständnis in der Rechtsprechung des Bundesverfassungsgerichts – Zur Rechtsprechung des Bundesverfassungsgerichts zu Art. 2 Abs. 2 Satz 1 GG, in: Berberich, Thomas/Holl, Wolfgang/Maaß, Kurt-Jürgen (Hrsg.), Neue Entwicklungen im öffentlichen Recht – Beiträge zum Verhältnis von Bürger und Staat aus Völkerrecht, Verfassungsrecht und Verwaltungsrecht; Tagungsbeiträge eines Symposiums der Alexander von Humboldt-Stiftung, Bonn-Bad Godesberg, veranstaltet vom 10. bis 14. Oktober 1978 in Ludwigsburg, Stuttgart u. a. 1979, 255–279.
Steinmüller, Wilhelm, Informationsrecht und Informationspolitik, in: ders. (Hrsg.), Informationsrecht und Informationspolitik, München, Wien 1976, 1–20.

Steinmüller, Wilhelm/Lutterbeck, Bernd/Mallmann, Christoph/Harbort, U./Kolb, Gerhard./Schneider, Jochen, Grundfragen des Datenschutzes. Gutachten im Auftrag des Bundesministeriums des Inneren, Bonn 7.1971.

Stern, Das Staatsrecht der Bundesrepublik Deutschland III/1. Allgemeine Lehren der Grundrechte; Grundlagen und Geschichte, nationaler und internationaler Grundrechtskonstitutionalismus, juristische Bedeutung der Grundrechte, Grundrechtsberechtigte, Grundrechtsverpflichtete, München 1988.

Stern, Klaus, Der allgemeine Privatsphärenschutz durch das Grundgesetz und seine Parallelen im internationalen und europäischen Recht, in: Bröhmer, Jürgen/Bieber, Roland/Calliess, Christian/Langenfeld, Christine/Weber, Stefan/Wolf, Joachim (Hrsg.), Internationale Gemeinschaft und Menschenrechte – Festschrift für Georg Ress zum 70. Geburtstag am 21. Januar 2005, Köln u. a. 2005, 1259–1276.

–, Die Schutzpflichtenfunktion der Grundrechte. Eine juristische Entdeckung, DÖV 2010, 241–249.

Strahilevitz, Lior Jacob, Towards a Positive Theory of Privacy Law, 126 Harvard L. Rev. (2013), 2010–2042.

Streinz, Rudolf, Die Rechtsprechung des EuGH zum Datenschutz, DuD 2011, 602–606.

Streinz, Rudolf/Michl, Walther, Die Drittwirkung des europäischen Datenschutzgrundrechts (Art. 8 GRCh) im deutschen Privatrecht, EuZW 2011, 384–388.

Streuer, Wibke, Die positiven Verpflichtungen des Staates. Eine Untersuchung der positiven Verpflichtungen des Staates aus den Grund- und Menschenrechten des Grundgesetzes und der Europäischen Menschenrechtskonvention, Baden-Baden 2003.

Strohmeier, Gerd, Politik und Massenmedien. Eine Einführung, Baden-Baden 2004.

Sunstein, Cass R., The Storrs Lectures: Behaviour Economics and Paternalism, 122 Yale L. J. (2013), 1826–1899.

–, Nudges, Agency, and Abstraction. A Reply to Critics, 6 Rev. of Philosophy and Psychology (2015), 511–529.

Sunstein, Cass R./Thaler, Richard H., Libertarian Paternalism is Not an Oxymoron, 70 Chicago L. Rev. (2003), 1159–1202.

Talidou, Zoi, Regulierte Selbstregulierung im Bereich des Datenschutzes, Frankfurt am Main 2005.

Teifke, Nils, Das Prinzip Menschenwürde. Zur Abwägungsfähigkeit des Höchstrangigen, Tübingen 2011.

Tene, Omer/Wolf, Christopher, Overextended: Jurisdiction and Applicable Law under the EU General Data Protection Regulation. White Paper 2.2013, http://www.futureofprivacy.org/wp-content/uploads/FINAL-Future-of-Privacy-Forum-White-Paper-on-Jurisdiction-and-Applicable-Law-January-20134.pdf.

Thaler, Richard H./Sunstein, Cass R., Libertarian Paternalism, 93 AEA Papers and Proceedings (2003), 175–179.

–/–, Nudge. Wie man kluge Entscheidungen anstößt, 2. Aufl., Berlin 2012.

The Pew Research Center for the People & the Press, Americans Spending More Time Following the News. Ideological News Sources: Who Watches and Why, Washington 12.9.2010, http://www.people-press.org/files/legacy-pdf/652.pdf.

The White House, Consumer Data Privacy in a Networked World. A Framework for Protecting Privacy and Promoting Innovation in the Global Digital Economy, Washington 2.2012.

Thomé, Sarah, Zweiter Teil, in: Kutscha, Martin/Thomé, Sarah (Hrsg.), Grundrechtsschutz im Internet?, Baden-Baden 2013, 101–135.

Thomson, Judith Jarvis, The Right to Privacy, 4 Philosophy & Public Affairs (1975), 295–314.

Thüsing, Gregor (Hrsg.), Beschäftigtendatenschutz und Compliance. Effektive Compliance im Spannungsfeld von BDSG, Persönlichkeitsschutz und betrieblicher Mitbestimmung, 2. Aufl., München 2014.

Tian, Lichun, Objektive Grundrechtsfunktionen im Vergleich. Eine Untersuchung anhand des Grundgesetzes und der Europäischen Menschenrechtskonvention, Berlin 2012.

Tinnefeld, Marie Theres, Geschützte Daten, in: Roßnagel, Alexander (Hrsg.), Handbuch Datenschutzrecht – Die neuen Grundlagen für Wirtschaft und Verwaltung, München 2003, 485–500.

Trepte, Sabine, Privatsphäre aus psychologischer Sicht, in: Schmidt, Jan-Hinrik/Weichert, Thilo (Hrsg.), Datenschutz – Grundlagen, Entwicklungen und Kontroversen, Bonn 2012, 59–65.

Trepte, Sabine/Dienlin, Tobias/Reinecke, Leonard, Privacy, Self-Disclosure, Social Support, and Social Network Site Use. Research Report of a Three-Year Panel Study, 29.10.2013, http://opus.uni-hohenheim.de/volltexte/2013/889/pdf/Trepte_Dienlin_Reinecke_2013_Privacy_Self_Disclosure_Social_Support_and_SNS_Use.pdf.

Trute, Hans-Heinrich, Verfassungsrechtliche Grundlagen, in: Roßnagel, Alexander (Hrsg.), Handbuch Datenschutzrecht – Die neuen Grundlagen für Wirtschaft und Verwaltung, München 2003, 156–187.

Tsai, Janice Y./Egelman, Serge/Cranor, Lorrie Faith/Acquisti, Alessandro, The Effect of Online Privacy Information on Purchasing Behavior: An Experimental Study, 22 Information Systems Research (2011), 254–268.

Uerpmann-Wittzack, Robert/Jankowska-Gilberg, Magdalena, Die Europäische Menschenrechtskonvention als Ordnungsrahmen für das Internet, MMR 2008, 83–89.

Uhle, Arnd, Freiheitlicher Verfassungsstaat und kulturelle Identität, Tübingen 2004.

Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein, Selbstregulierung bei „Do Not Track“ gescheitert. ULD: „Gefordert sind nun Politik und Aufsicht“, Kiel 19.10.2012, https://www.datenschutzzentrum.de/presse/20121019-selbstregulierung-do-not-track.htm.

Unseld, Christopher, Mehr Schutzpflicht wagen? In den USA beschäftigt die Abtreibungsfrage erneut die Gerichte, 4.9.2014, http://www.verfassungsblog.de/mehr-schutzpflicht-wagen-den-usa-beschaeftigt-die-abtreibungsfrage-erneut-die-gerichte/#.VAiwK2NDXNA.

van Aaken, Anne, Begrenzte Rationalität und Paternalismusgefahr: Das Prinzip des schonendsten Paternalismus, in: Anderheiden, Michael/Bürkli, Peter/Heinig, Hans Michael/Kirste, Stephan/Seelmann, Kurt (Hrsg.), Paternalismus und Recht – In memoriam Angela Augustin (1968–2004), Tübingen 2006, 109–144.

–, Das deliberative Element juristischer Verfahren als Instrument zur Überwindung nachteiliger Verhaltensanomalien – Ein Plädoyer für die Einbezieung diskursiver Elemente in die Verhaltensökonomik des Rechts, in: Engel, Christoph/Englerth, Markus/Lüdemann, Jörn/Spiecker genannt Döhmann, Indra (Hrsg.), Recht und Verhalten – Beiträge zu Behavioral Law and Economics, Tübingen 2007, 189–230.

van Hoboken, Joris, Search engine freedom: on the implications of the right to freedom of expression for the legal governance of Web search engines, Amsterdam 2012, http://dare.uva.nl/document/357527.

Volkmann, Uwe, Darf der Staat seine Bürger erziehen?, Baden-Baden 2012.

Vossenkuhl, Wilhelm, Gerechtigkeit, Paternalismus und Vertrauen, in: Fateh-Moghadam, Bijan/Sellmaier, Stephan/Vossenkuhl, Wilhelm (Hrsg.), Grenzen des Paternalismus, Stuttgart 2010, 163–181.

Wagner, Edgar, Datenschutz als Bildungsaufgabe, in: Schmidt, Jan-Hinrik/Weichert, Thilo (Hrsg.), Datenschutz – Grundlagen, Entwicklungen und Kontroversen, Bonn 2012, 88–98.

–, Datenschutz als Bildungsauftrag, DuD 2012, 83–87.

–, Digitale Aufklärung – Medienkompetenz als Bildungsaufgabe, in: Hill, Hermann/Martini, Mario/Wagner, Edgar (Hrsg.), Facebook, Google & Co. – Chancen und Risiken, Baden-Baden 2013, 143–150.

Wahl, Rainer/Masing, Johannes, Schutz durch Eingriff, JZ 1990, 553–563.

Wang, Yang/Leon, Pedro Giovanni/Chen, Xiaoxuan/Komanduri, Saranga/Norcie, Gregory/Scott, Kevin/Acquisti, Alessandro/Cranor, Lorrie Faith/Sadeh, Norman, From Facebook Regrets to Facebook Privacy Nudges, 74 Ohio State L. J. (2013), 1307–1334.

Warren, Samuel D./Brandeis, Louis D., The Right to Privacy, 4 Harvard L. Rev. (1890), 193–220.

Weber, Klaus (Hrsg.), Betäubungsmittelgesetz. Arzneimittelgesetz. Kommentar, 4. Aufl. 2013.

Weichert, Thilo, Die Ökonomisierung des Rechts auf informationelle Selbstbestimmung, NJW 2001, 1463–1469.

–, Datenschutz als Verbraucherschutz. Anforderungen und Haltungen der Nutzenden, in: Peissl, Walter (Hrsg.), Privacy – Ein Grundrecht mit Ablaufdatum?, Wien 2003, 145–154.

–, Datenschutz im Wettbewerbs- und Verbraucherrecht, VuR 2006, 377–383.

–, Privatheit und Datenschutz im Konflikt zwischen den USA und Europa, RDV 2012, 113–118.

Weidner-Braun, Ruth, Der Schutz der Privatsphäre und des Rechts auf informationelle Selbstbestimmung. am Beispiel des personenbezogenen Datenverkehrs im WWW nach deutschem öffentlichen Recht, Berlin 2012.

Welchering, Peter, Vom überwachten Bürger zum gläsernen Menschen – Big-Data-Analysen führen zu verblüffenden und teilweise gefährlichen Ergebnissen, DANA 2014, 144–146.

Westin, Alan F., Privacy and Freedom, New York 1967.

Whitman, James Q., The Two Western Cultures of Privacy: Dignity Versus Liberty, 113 Yale L. J. (2004), 1151–1221.

Wielpütz, Saskia, Über das Recht, ein anderer zu werden und zu sein. Verfassungsrechtliche Probleme des Transsexuellengesetzes, Baden-Baden 2012.

Wieser, Bernd, Vergleichendes Verfassungsrecht, Wien/New York 2005.

Wietfeld, Dominik, Selbstbestimmung und Selbstverantwortung – Die gesetzliche Regelung der Patientenverfügung, Baden-Baden 2012.

Wilkens, Andreas, Bericht: Schufa will Daten in sozialen Netzwerken nutzen, 7.6.2012, http://www.heise.de/newsticker/meldung/Bericht-Schufa-will-Daten-in-sozialen-Netzwerken-nutzen-1612450.html.

Willis, Lauren E., When Nudges Fail: Slippery Defaults, 80 Chicago L. Rev. (2013), 1115–1129.

–, Why not Privacy by Default?, 29 Berkeley Tech. L. J. (2014).

Wittern, Felix, Das Verhältnis von Right of Privacy und Persönlichkeitsrecht zur Freiheit der Massenmedien. Eine rechtsvergleichende Darstellung des Verhältnisses von Right of Privacy und Persönlichkeitsrecht zu der Redefreiheit in den Vereinigten Staaten von Amerika und der Presse- und Rundfunkfreiheit in Deutschland, Hamburg 2004.

Wittmann, Philipp, Der Schutz der Privatsphäre vor staatlichen Überwachungsmaßnahmen durch die US-amerikanische Bundesverfassung. Eine Untersuchung unter besonderer Berücksichtigung des Schutzes der Privatsphäre in der Öffentlichkeit, Baden-Baden 2014.

Wolff, Heinrich A., Privatheit und Öffentlichkeit – eine Positionsbestimmung in der digitalen Welt, in: Hill, Hermann/Martini, Mario/Wagner, Edgar (Hrsg.), Facebook, Google & Co. – Chancen und Risiken, Baden-Baden 2013, 19–32.

Worms, Christoph/Gusy, Christoph, Verfassung und Datenschutz. Das Private und das Öffentliche in der Rechtsordnung, DuD 2012, 92–99.

Wu, Felix T., The Commercial Difference. Draft for the 7th Privacy Law Scholars Conference, Washington 18.5.2014, vgl. http://isp.yale.edu/sites/default/files/page-attachments/Felix%20Wu%20-%20The%20Commercial%20Difference%20-%20FESC.pdf.

Würkner, Prostitution und Menschenwürdeprinzip. Reflexionen über die Ethisierung des Rechts am Beispiel des gewerblichen Ordnungsrechts, NVwZ 1988, 600–602.

Xenos, Dimitris, The Positive Obligations of the State under the European Convention of Human Rights, London/New York 2012.

Yoo, Christopher, Free Speech and the Myth of the Internet as an Unintermediated Experience, 78 George Washington L. Rev. (2010), 697–773.

–, When Antitrust Met Facebook, 19 George Mason L. Rev. (2012), 1147–1162.

Zeidler, Simon Alexander/Brüggemann, Sebastian, Die Zukunft personalisierter Werbung im Internet, CR 2014, 248–257.

Zezschwitz, Friedrich v., Konzepte der normativen Zweckbegrenzung, in: Roßnagel, Alexander (Hrsg.), Handbuch Datenschutzrecht – Die neuen Grundlagen für Wirtschaft und Verwaltung, München 2003, 219–268.

Zimmeck, Sebastian/Bellovin, Steven M., Privee: An Architecture for Automatically Analyzing Web Privacy Policies, in: Proceedings of the 23rd USENIX Security Symposium, San Diego 2014, 1–16.

Zscherpe, Kerstin, Anforderungen an die datenschutzrechtliche Einwilligung im Internet, MMR 2004, 723–727.

Zuiderveen Borgesius, Frederik, Consent to Behavioural Targeting in European Law. What are the Policy Implications to Insights from Behavioural Economics? Draft for the 6th Privacy Law Scholars Conference, Berkeley 7.2013.

–, Improving Privacy Protection in the Area of Behavioural Targeting, Dordrecht 2015.

Register